Computers and Mathematics with Applications 60 (2010) 2983–2997

Contents lists available at ScienceDirect

Computers and Mathematics with Applications

journal homepage: www.elsevier.com/locate/camwa

Decomposing polynomial sets into simple sets over finite fields: The zero-dimensional case

Xiaoliang Li [a,*], Chenqi Mou [a,b], Dongming Wang [b]

[a] LMIB – SKLSDE – School of Mathematics and Systems Science, Beihang University, Beijing 100191, China

[b] Laboratoire d'Informatique de Paris 6, Université Pierre et Marie Curie – CNRS, 104 avenue du Président Kennedy, F-75016 Paris, France

ARTICLE INFO

Article history:
Received 2 July 2009
Received in revised form 26 September 2010
Accepted 28 September 2010

Keywords:
Simple set
Finite field
Regular set
Squarefree decomposition
*p*th root extraction

ABSTRACT

This paper presents algorithms for decomposing any zero-dimensional polynomial set into simple sets over an arbitrary finite field, with an associated ideal or zero decomposition. As a key ingredient of these algorithms, we generalize the squarefree decomposition approach for univariate polynomials over a finite field to that over the field product determined by a simple set. As a subprocedure of the generalized squarefree decomposition approach, a method is proposed to extract the *p*th root of any element in the field product. Experiments with a preliminary implementation show the effectiveness of our algorithms.

1. Introduction

Polynomial systems occur in many domains of science and engineering, from coding theory [1] and cryptography [2] to biological modeling [3]. The method of triangular sets provides a computational tool for the study of polynomial systems [4–7]. There are several algorithms which can decompose any set of multivariate polynomials into triangular sets with different properties [8–14]. The properties reveal the inherent structure of the original polynomial set and make the method applicable to diverse problems (e.g., proving geometric theorems [15] and solving algebraic equations [8,9]).

Although triangular sets over fields of characteristic 0 have been extensively studied and most of the algorithms proposed (e.g., those in [10,11,13]) work also in the finite field case, there are some exceptions. For example, the decomposition of a given polynomial set into simple systems or sets [12] or squarefree regular chains [16,6] over finite fields is a nontrivial task, but is of theoretical interest. Simple sets possess the property of squarefreeness, their saturated ideals are radical, and with them radical ideal membership can be tested by using pseudo-division. The present study is a first step towards the development of efficient algorithms for the computation of simple sets over finite fields.

The paper first recalls the definition of simple sets over arbitrary fields in an algebraic way and then proves relevant properties. Aiming at designing algorithms to decompose zero-dimensional polynomial sets into simple sets over finite fields, we generalize the squarefree decomposition approach for univariate polynomials over a finite field to that over the field product determined by a simple set. In this generalization, *p*th root extraction in the field product is a key ingredient. An approach is proposed to compute the *p*th root by recursively solving linear equations. Based

* Corresponding address: DYC-2-910A, No. 29 Zhichun Road, Haidian District, Beijing 100083, China. Mobile: +86 13810480701.
E-mail addresses: xiaoliangbuaa@gmail.com (X. Li), chenqi.mou@gmail.com (C. Mou), dongming.wang@lip6.fr (D. Wang).

0898-1221/$ – see front matter © 2010 Elsevier Ltd. All rights reserved.
doi:10.1016/j.camwa.2010.09.059

on this approach, we present algorithms to decompose any zero-dimensional polynomial set into simple sets over an arbitrary finite field. These algorithms can produce both ideal and zero decompositions of the given polynomial set. Furthermore, a simple decomposition method with a zero relation in the ground field is also proposed by making use of the properties of finite fields. Our experiments with a preliminary implementation show that the algorithms are effective.

The paper is structured as follows. In Section 2, basic concepts about triangular sets and regular sets are reviewed. In Section 3, the definition and properties of simple sets are given. Section 4 addresses generalized squarefree decomposition in the zero-dimensional case, including pth root extraction in any field product. Algorithms to decompose polynomial sets into simple sets over finite fields are presented in Section 5. Section 6 provides experimental results with our implementation.

2. Preliminaries

2.1. Triangular sets

Let $\mathcal{K}$ be a field and $\mathcal{K}[x_1, \ldots, x_n]$ be the ring of polynomials in the variables x_i with a fixed order $x_1 < \cdots < x_n$. We use $\boldsymbol{x}$ and $\boldsymbol{x}_i$ to denote $x_1, \ldots, x_n$ and $x_1, \ldots, x_i$ respectively.

For any polynomial $F \in \mathcal{K}[\boldsymbol{x}]$ and variable x_k, we denote by $\deg(F, x_k)$ the *degree* of F in x_k and by $\mathrm{lc}(F, x_k)$ the *leading coefficient* of F with respect to (w.r.t.) x_k. The biggest variable effectively appearing in F is called the *leading variable* of F and denoted by $\mathrm{lv}(F)$. Suppose that $\mathrm{lv}(F) = x_p$. Considered as a polynomial in $\mathcal{K}[\boldsymbol{x}_{p-1}][x_p]$, F can be written as $F = Ix_p^d + R$, where $\deg(R, x_p) < d$. We call I, d, and R the *initial*, *leading degree*, and *reductum* of P and denote them by $\mathrm{ini}(F)$, $\mathrm{ldeg}(F)$, and $\mathrm{red}(F)$ respectively.

For two nonzero polynomials $F, G \in \mathcal{K}[\boldsymbol{x}]$ with $\deg(F, x_k) = m$ and $\deg(G, x_k) = l > 0$, the pseudo-division algorithm computes two polynomials $Q, R \in \mathcal{K}[\boldsymbol{x}]$ such that $I^q F = QG + R$, where $I = \mathrm{lc}(G, x_k)$, $q = \max(m - l + 1, 0)$, $\deg(Q, x) = \max(m - l, -1)$, and $\deg(R, x_k) < l$. The polynomials Q and R are called the *pseudo-quotient* and *pseudo-remainder* of F w.r.t. G in x_k and denoted by $\mathrm{pquo}(F, G, x_k)$ and $\mathrm{prem}(F, G, x_k)$ respectively. If $\mathrm{lv}(G) = x_k$, then $\mathrm{prem}(F, G) := \mathrm{prem}(F, G, x_k)$ and $\mathrm{pquo}(F, G) := \mathrm{pquo}(F, G, x_k)$.

Definition 2.1. A polynomial set $\mathcal{T} \subseteq \mathcal{K}[\boldsymbol{x}]$ is called a *triangular set* if

(a) $\mathcal{T} \cap \mathcal{K} = \emptyset$;
(b) for any two distinct polynomials $F, G \in \mathcal{T}$, $\mathrm{lv}(F) \neq \mathrm{lv}(G)$.

For any triangular set $\mathcal{T} \subseteq \mathcal{K}[\boldsymbol{x}]$, if a variable appears as the leading variable of some $T \in \mathcal{T}$, then it is called a *dependent* of $\mathcal{T}$; otherwise it is called a *parameter* of $\mathcal{T}$. If $\mathcal{T}$ does not contain any parameter, then it is said to be *zero-dimensional*. Rename all the dependents of $\mathcal{T}$ as $y_1 < \cdots < y_r$ and all the parameters of $\mathcal{T}$ as $u_1 < \cdots < u_t$, where $r + t = n$. The variables $u_1, \ldots, u_t$ are denoted by $\boldsymbol{u}$. It is then easy to know that $\mathcal{T}$ is still a triangular set under the variable order $u_1 < \cdots < u_t < y_1 < \cdots < y_r$. Without loss of generality, we will always assume that the parameters are ordered smaller than the dependents.

The triangular set $\mathcal{T}$ can be written in order as $\mathcal{T} = [T_1, \ldots, T_r]$, with $\mathrm{lv}(T_j) = y_i$ for $i = 1, \ldots, r$. We use the notations $\mathcal{T}_{<i} := [T_1, \ldots, T_{i-1}]$ and $\mathcal{T}_{\leq i} := [T_1, \ldots, T_i]$. The *pseudo-remainder* $\mathrm{prem}(F, \mathcal{T})$ of any polynomial $F \in \mathcal{K}[\boldsymbol{x}]$ w.r.t. $\mathcal{T}$ is defined recursively as $\mathrm{prem}(\mathrm{prem}(F, T_r), \mathcal{T}_{<r})$, where $\mathrm{prem}(F, \emptyset) := F$. The polynomial F is said to be *reduced* w.r.t. $\mathcal{T}$ if $\deg(F, y_i) < \mathrm{ldeg}(T_i)$ for all $i = 1, \ldots, r$. Obviously, $\mathrm{prem}(F, \mathcal{T})$ is reduced w.r.t. $\mathcal{T}$. We use $\mathrm{res}(F, G)$ to denote the resultant of any two polynomials $F, G \in \mathcal{K}[\boldsymbol{x}]$ w.r.t. $\mathrm{lv}(G)$ and recursively define $\mathrm{res}(F, \mathcal{T}) := \mathrm{res}(\mathrm{res}(F, T_r), \mathcal{T}_{<r})$, where $\mathrm{res}(F, \emptyset) := F$.

Let $\tilde{\mathcal{K}}$ be the transcendental extension field $\mathcal{K}(\boldsymbol{u})$ and $\boldsymbol{y}_i$ stand for $y_1, \ldots, y_i$ with $\boldsymbol{y} = \boldsymbol{y}_r$. To avoid ambiguity, for any ideal $\mathfrak{a} \subseteq \mathcal{K}[\boldsymbol{u}][\boldsymbol{y}_i]$, we use $\mathfrak{a}_{\tilde{\mathcal{K}}}$ to denote the ideal generated by $\mathfrak{a}$ in $\tilde{\mathcal{K}}[\boldsymbol{y}_i]$. Let H be the product of all the initials of the polynomials in $\mathcal{T}$. The *saturated ideal* of $\mathcal{T}$ is defined as $\mathrm{sat}(\mathcal{T}) := \langle \mathcal{T} \rangle : H^\infty$. Then $\mathrm{sat}_i(\mathcal{T}) := \mathrm{sat}(\mathcal{T}_{\leq i})$ is an ideal in $\mathcal{K}[\boldsymbol{u}][\boldsymbol{y}_i]$. It is necessary to mention that the notation sat_i here is slightly different from that in [4].

2.2. Regular sets

Let $\mathcal{R}$ be a commutative ring with unit and $\mathfrak{a}$ an ideal in $\mathcal{R}$. Then $P \in \mathcal{R}$ is said to be *regular* in $\mathcal{R}$ if P is neither zero, nor a zero divisor in $\mathcal{R}$, and *regular modulo* $\mathfrak{a}$ if P is regular in $\mathcal{R}/\mathfrak{a}$.

Definition 2.2. Let $\mathcal{T} = [T_1, \ldots, T_r] \subseteq \mathcal{K}[\boldsymbol{x}]$ be a triangular set. $\mathcal{T}$ is called a *regular set* in $\mathcal{K}[\boldsymbol{x}]$ if for all $i = 1, \ldots, r$, $\mathrm{ini}(T_i)$ is regular modulo $\mathrm{sat}_{i-1}(\mathcal{T})$.

Regular set was introduced first in [10] as regular chain and in [17] as proper ascending chain. Our notion follows [4,13].

In the following, we first review the Chinese remainder theorem in algebra [18], which plays an important role in this paper, and then list several well-known properties of regular sets.

Theorem 2.1 (*Chinese Remainder Theorem*). *Let* $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ *be ideals in* $\mathcal{R}$ *such that* $\mathfrak{a}_i + \mathfrak{a}_j = \mathcal{R}$ *for all* $i \neq j$. *Then*

$$\mathcal{R}/\left(\bigcap_{i=1}^{r} \mathfrak{a}_i\right) \cong \prod_{i=1}^{r} \mathcal{R}/\mathfrak{a}_i.$$

As the theorem states, if $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ are all maximal ideals in $\mathcal{R}$, then each $\mathcal{R}/\mathfrak{a}_i$ is a field for $i = 1, \ldots, r$. In this case, $\mathcal{R}/\left(\bigcap_{i=1}^{r} \mathfrak{a}_i\right)$ is isomorphic to a product of fields.

Proposition 2.2 (*[4, Theorem 6.1], [13, Theorem 5.1]*). *For any regular set* $\mathcal{T} \subseteq \mathcal{K}[\boldsymbol{x}]$ *and polynomial* $P \in \mathcal{K}[\boldsymbol{x}]$,

(a) $P \in \mathrm{sat}(\mathcal{T})$ *if and only if* $\mathrm{prem}(P, \mathcal{T}) = 0$;
(b) P *is regular modulo* $\mathrm{sat}(\mathcal{T})$ *if and only if* $\mathrm{res}(P, \mathcal{T}) \neq 0$.

Proposition 2.3 (*[6, Theorem 4.4]*). *Let* $\mathcal{T}$ *be a regular set in* $\mathcal{K}[\boldsymbol{x}]$. *Then*

(a) $\mathrm{sat}(\mathcal{T}) \neq \langle 1 \rangle$;
(b) $\mathrm{sat}(\mathcal{T})$ *is unmixed-dimensional and its parameters form a transcendental basis of every associated prime of* $\mathrm{sat}(\mathcal{T})$.

Proposition 2.4 (*[6, Proposition 5.8]*). *Let* $\mathcal{T}$ *be a regular set in* $\mathcal{K}[\boldsymbol{x}]$. *Then* $\mathcal{T}_{\leq i}$ *is a regular set in* $\mathcal{K}[\boldsymbol{u}][\boldsymbol{y}_i]$ *and for any dependent* y_i *of* $\mathcal{T}$,

(a) $\mathrm{sat}_i(\mathcal{T}) = \mathrm{sat}(\mathcal{T}) \cap \mathcal{K}[\boldsymbol{u}][\boldsymbol{y}_i]$;
(b) *the associated primes of* $\mathrm{sat}_i(\mathcal{T})$ *are the intersections of the associated primes of* $\mathrm{sat}(\mathcal{T})$ *with* $\mathcal{K}[\boldsymbol{u}][\boldsymbol{y}_i]$.

For any regular set $\mathcal{T}$, Proposition 2.2 indicates that the membership in the saturated ideal $\mathrm{sat}(\mathcal{T})$ and the regularity modulo $\mathrm{sat}(\mathcal{T})$ can be easily tested. Proposition 2.3 shows that $\mathrm{sat}(\mathcal{T})$ is nontrivial and unmixed-dimensional, and Proposition 2.4 shows its cutback properties. Recall that $\mathrm{sat}_i(\mathcal{T})_{\tilde{\mathcal{K}}}$ is the ideal generated by $\mathrm{sat}_i(\mathcal{T})$ in $\tilde{\mathcal{K}}[\boldsymbol{y}_i]$. Computing the localization of the formula in Proposition 2.4(a) at $\mathcal{K}[\boldsymbol{u}] \setminus \{0\}$, we have $\mathrm{sat}_i(\mathcal{T})_{\tilde{\mathcal{K}}} = \mathrm{sat}(\mathcal{T})_{\tilde{\mathcal{K}}} \cap \tilde{\mathcal{K}}[\boldsymbol{y}_i]$. More about $\mathrm{sat}_i(\mathcal{T})_{\tilde{\mathcal{K}}}$: the following property plays a key role in this paper.

Proposition 2.5 (*[6, Proposition 5.18]*). *For any regular set* $\mathcal{T} \subseteq \mathcal{K}[\boldsymbol{x}]$, $\mathrm{sat}_i(\mathcal{T})_{\tilde{\mathcal{K}}} = \langle \mathcal{T}_{\leq i} \rangle_{\tilde{\mathcal{K}}}$.

3. Simple sets

In this section, we first clarify the definition of simple sets over arbitrary fields and then prove relevant properties. A simple decomposition algorithm for the characteristic 0 case is reviewed in preparation for later discussions.

3.1. Definitions and properties

In what follows, $\mathcal{K}$ is an arbitrary field unless otherwise specified. Let $\mathcal{T} = [T_1, \ldots, T_r]$ be a regular set in $\mathcal{K}[\boldsymbol{x}]$ with $\mathrm{lv}(T_i) = y_i$ $(1 \leq i \leq r)$ and F be a polynomial in $\mathcal{K}[\boldsymbol{u}][\boldsymbol{y}_i]$, which can also be viewed as an element in $\tilde{\mathcal{K}}[\boldsymbol{y}_i]$. For any prime ideal $\mathfrak{p} \subseteq \tilde{\mathcal{K}}[\boldsymbol{y}_{i-1}]$, $\overline{F}^{\mathfrak{p}}$ denotes the image of F in $(\tilde{\mathcal{K}}[\boldsymbol{y}_{i-1}]/\mathfrak{p})[y_i]$ under the natural homomorphism. Let $\mathcal{P}$ be a polynomial set in $\tilde{\mathcal{K}}[\boldsymbol{y}_i]$. We define $\overline{\mathcal{P}}^{\mathfrak{p}} := \{\overline{P}^{\mathfrak{p}} : P \in \mathcal{P}\}$. Moreover, $\overline{F}$ denotes the image of F in $(\tilde{\mathcal{K}}[\boldsymbol{y}_{i-1}]/\sqrt{\mathrm{sat}_{i-1}(\mathcal{T})_{\tilde{\mathcal{K}}}})[y_i]$ if no ambiguity occurs, and $\overline{\mathcal{P}}$ is similarly defined. For any ideal $\mathfrak{a} = \langle P_1, \ldots, P_s \rangle \subseteq \tilde{\mathcal{K}}[\boldsymbol{y}_i]$, one can verify that $\overline{\mathfrak{a}}^{\mathfrak{p}} = \langle \overline{P}_1^{\mathfrak{p}}, \ldots, \overline{P}_s^{\mathfrak{p}} \rangle$ and $\overline{\mathfrak{a}} = \langle \overline{P}_1, \ldots, \overline{P}_s \rangle$.

Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ be all the associated primes of $\mathrm{sat}_{i-1}(\mathcal{T})_{\tilde{\mathcal{K}}}$. As $\mathcal{T}$ is unmixed-dimensional, we know that all its associated primes are isolated, i.e. for all $j \neq k$, $\mathfrak{p}_j \not\subseteq \mathfrak{p}_k$ and thus $\mathfrak{p}_j + \mathfrak{p}_k = \langle 1 \rangle$. By the Chinese remainder theorem, $\tilde{\mathcal{K}}[\boldsymbol{y}_{i-1}]/\sqrt{\mathrm{sat}_{i-1}(\mathcal{T})_{\tilde{\mathcal{K}}}} \cong \prod_{j=1}^{s} \tilde{\mathcal{K}}[\boldsymbol{y}_{i-1}]/\mathfrak{p}_j$. It should be noted that $\mathrm{sat}_{i-1}(\mathcal{T})_{\tilde{\mathcal{K}}}$ is a zero-dimensional ideal in $\tilde{\mathcal{K}}[\boldsymbol{y}_{i-1}]$, so every $\mathfrak{p}_j$ is maximal and hence $\tilde{\mathcal{K}}[\boldsymbol{y}_{i-1}]/\mathfrak{p}_j$ is a field. Consequently, one can prove that

$$(\tilde{\mathcal{K}}[\boldsymbol{y}_{i-1}]/\sqrt{\mathrm{sat}_{i-1}(\mathcal{T})_{\tilde{\mathcal{K}}}})[y_i] \cong \prod_{j=1}^{s} (\tilde{\mathcal{K}}[\boldsymbol{y}_{i-1}]/\mathfrak{p}_j)[y_j]. \tag{1}$$

We do not distinguish between elements in the two isomorphic rings above; thus $\overline{F} = (\overline{F}^{\mathfrak{p}_1}, \ldots, \overline{F}^{\mathfrak{p}_s})$ for any $F \in \tilde{\mathcal{K}}[\boldsymbol{y}_i]$. The projection $\pi_j : (\tilde{\mathcal{K}}[\boldsymbol{y}_{i-1}]/\sqrt{\mathrm{sat}_{i-1}(\mathcal{T})_{\tilde{\mathcal{K}}}})[y_i] \to (\tilde{\mathcal{K}}[\boldsymbol{y}_{i-1}]/\mathfrak{p}_j)[y_i]$ is defined as $\pi_j(\overline{F}) = \overline{F}^{\mathfrak{p}_j}$ for $j = 1, \ldots, s$. It is easy to prove that an ideal $\mathfrak{b}$ in $(\tilde{\mathcal{K}}[\boldsymbol{y}_{i-1}]/\sqrt{\mathrm{sat}_{i-1}(\mathcal{T})_{\tilde{\mathcal{K}}}})[y_i]$ is radical if and only if $\pi_j(\mathfrak{b})$ is a radical ideal for all $j = 1, \ldots, s$.

Definition 3.1. Let $\mathcal{T} = [T_1, \ldots, T_r]$ be a regular set in $\mathcal{K}[\boldsymbol{x}]$ with $\mathrm{lv}(T_i) = y_i$ $(1 \le i \le r)$. It is called a *simple set* or said to be *simple* if for any $i = 1, \ldots, r$ and associated prime $\mathfrak{p}$ of $\mathrm{sat}_{i-1}(\mathcal{T})_{\tilde{\mathcal{K}}}$, $\overline{T}_i^{\mathfrak{p}}$ is a squarefree polynomial in $(\tilde{\mathcal{K}}[\boldsymbol{y}_{i-1}]/\mathfrak{p})[y_i]$.

The notion of simple set originates from [19,12] and is equivalent to that of *squarefree regular chain* used in [6]. Most of the results presented below for an arbitrary field $\mathcal{K}$ are refined or reproduced from [6], where the field of interest is of characteristic 0. Thus the properties about simple sets stated in this section are somewhat more general than those in [6].

Lemma 3.1. *Let $\mathcal{T} = [T_1, \ldots, T_r]$ be a regular set in $\mathcal{K}[\boldsymbol{x}]$ with $\mathrm{lv}(T_i) = y_i$ $(1 \le i \le r)$. Then $\overline{\mathrm{sat}_i(\mathcal{T})_{\tilde{\mathcal{K}}}} = \langle \overline{T}_i \rangle$ for all $i = 1, \ldots, r$.*

Proof. By Proposition 2.5, $\mathrm{sat}_i(\mathcal{T})_{\tilde{\mathcal{K}}} = \langle \mathcal{T}_{\le i} \rangle_{\tilde{\mathcal{K}}}$. For any $T \in \mathcal{T}_{\le i-1}$, we have $T \in \mathrm{sat}_{i-1}(\mathcal{T})_{\tilde{\mathcal{K}}} \subseteq \sqrt{\mathrm{sat}_{i-1}(\mathcal{T})_{\tilde{\mathcal{K}}}}$ and thus $\overline{T} = 0$. The conclusion follows. □

Lemma 3.2. *Let $\mathcal{T} = [T_1, \ldots, T_r]$ be a regular set in $\mathcal{K}[\boldsymbol{x}]$ and $F \in \mathcal{K}[\boldsymbol{x}]$ with $\mathrm{lv}(F) = y_i$ $(1 \le i \le r)$. If $\overline{F} \in \langle \overline{T}_i \rangle$ and $\mathrm{sat}_{i-1}(\mathcal{T})_{\tilde{\mathcal{K}}}$ is radical, then $F \in \mathrm{sat}_i(\mathcal{T})_{\tilde{\mathcal{K}}}$.*

Proof. From the pseudo-division of F w.r.t. $\mathcal{T}_{\le i}$, we get $MF = \sum_{j=1}^{i-1} Q_j T_j + Q_i T_i + R$, where $R = \mathrm{prem}(F, \mathcal{T}_{\le i})$, $M = \prod_{j=1}^{i} \mathrm{ini}(T_j)^{s_j}$, and s_j is a nonnegative integer. Hence $\overline{M}\,\overline{F} = \overline{Q}_i\,\overline{T}_i + \overline{R}$. If $\overline{F} \in \langle \overline{T}_i \rangle$, then $\overline{R} \in \langle \overline{T}_i \rangle$. Noting that $\deg(\overline{R}, y_i) < \deg(\overline{T}_i, y_i)$, we have $\overline{R} = 0$.

Write $R = \sum_{l=0}^{d} A_l y_i^l$, where $A_l \in \mathcal{K}[\boldsymbol{u}][\boldsymbol{y}_{i-1}]$. Then $\overline{R} = \sum_{l=0}^{d} \overline{A}_l y_i^l = 0$. It follows that $\overline{A}_l = 0$ for all $l = 0, \ldots, d$. Therefore, $A_l \in \sqrt{\mathrm{sat}_{i-1}(\mathcal{T})_{\tilde{\mathcal{K}}}} = \mathrm{sat}_{i-1}(\mathcal{T})_{\tilde{\mathcal{K}}}$, and thus $A_l \in \mathrm{sat}_{i-1}(\mathcal{T})$. By Proposition 2.2, we have $A_l = \mathrm{prem}(A_l, \mathcal{T}_{<i}) = 0$. Hence $R = 0$ and $F \in \mathrm{sat}_i(\mathcal{T})_{\tilde{\mathcal{K}}}$. □

Theorem 3.3. *Let $\mathcal{T} = [T_1, \ldots, T_r]$ be a regular set in $\mathcal{K}[\boldsymbol{x}]$. Then the following statements are equivalent.*

(a) *$\mathcal{T}$ is simple;*
(b) *$\mathrm{sat}(\mathcal{T})$ is radical;*
(c) *$\mathrm{sat}(\mathcal{T})_{\tilde{\mathcal{K}}}$ is radical;*
(d) *$\mathrm{sat}_i(\mathcal{T})$ is radical for all $i = 1, \ldots, r$;*
(e) *$\mathrm{sat}_i(\mathcal{T})_{\tilde{\mathcal{K}}}$ is radical for all $i = 1, \ldots, r$.*

Proof. (a) ⇔ (e). Obviously, (a) implies (e) for $i = 1$. Suppose that $\mathrm{sat}_{i-1}(\mathcal{T})_{\tilde{\mathcal{K}}}$ is radical. We want to prove that $\mathrm{sat}_i(\mathcal{T})_{\tilde{\mathcal{K}}}$ is also radical. As $\mathcal{T}$ is simple, for any associated prime $\mathfrak{p}$ of $\mathrm{sat}_{i-1}(\mathcal{T})_{\tilde{\mathcal{K}}}$, $\overline{T}_i^{\mathfrak{p}}$ is a squarefree polynomial and thus $\langle \overline{T}_i^{\mathfrak{p}} \rangle$ is radical in $(\tilde{\mathcal{K}}[\boldsymbol{y}_{i-1}]/\mathfrak{p})[y_i]$. Hence $\langle \overline{T}_i \rangle$ is radical in $(\tilde{\mathcal{K}}[\boldsymbol{y}_{i-1}]/\mathrm{sat}_{i-1}(\mathcal{T})_{\tilde{\mathcal{K}}})[y_i]$. If $\mathrm{sat}_i(\mathcal{T})_{\tilde{\mathcal{K}}}$ is not radical, then there exist a polynomial $G \in \tilde{\mathcal{K}}[\boldsymbol{y}_i]$ and some integer k such that $G^k \in \mathrm{sat}_i(\mathcal{T})_{\tilde{\mathcal{K}}}$, but $G \notin \mathrm{sat}_i(\mathcal{T})_{\tilde{\mathcal{K}}}$. Therefore, we have $(\overline{G})^k \in \langle \overline{T}_i \rangle$ and $\overline{G} \notin \langle \overline{T}_i \rangle$ by Lemmas 3.1 and 3.2. This is a contradiction.

If $\mathcal{T}$ is not simple, then let i be the smallest integer such that the condition in the definition of simple set does not hold, i.e. there exists an associated prime $\mathfrak{p}$ of $\mathrm{sat}_{i-1}(\mathcal{T})_{\tilde{\mathcal{K}}}$ (radical) such that $\overline{T}_i^{\mathfrak{p}}$ is not squarefree. In this case, $\overline{\mathrm{sat}_i(\mathcal{T})^{\mathfrak{p}}_{\tilde{\mathcal{K}}}} = \langle \overline{T}_i^{\mathfrak{p}} \rangle$ is not radical. Hence $\langle \overline{T}_i \rangle$ is not radical, and neither is $\mathrm{sat}_i(\mathcal{T})_{\tilde{\mathcal{K}}}$.

(e) ⇔ (d). If $\mathrm{sat}_i(\mathcal{T})_{\tilde{\mathcal{K}}}$ is radical, then obviously $\mathrm{sat}_i(\mathcal{T})$ is also radical as $\mathrm{sat}_i(\mathcal{T})_{\tilde{\mathcal{K}}} \cap \mathcal{K}[\boldsymbol{u}][\boldsymbol{y}_i] = \mathrm{sat}_i(\mathcal{T})$.

Suppose that $\mathrm{sat}_i(\mathcal{T})$ is radical and recall that $\mathrm{sat}_i(\mathcal{T})_{\tilde{\mathcal{K}}} = (\mathcal{K}[\boldsymbol{u}] \setminus \{0\})^{-1}\mathrm{sat}_i(\mathcal{T})$. For any $(F/G)^s = F^s/G^s \in \mathrm{sat}_i(\mathcal{T})_{\tilde{\mathcal{K}}}$, we have $F^s \in \mathrm{sat}_i(\mathcal{T})$ and $G^s \in \mathcal{K}[\boldsymbol{u}]$; hence $F \in \mathrm{sat}_i(\mathcal{T})$ and $G \in \mathcal{K}[\boldsymbol{u}]$. Consequently, $F/S \in \mathrm{sat}_i(\mathcal{T})_{\tilde{\mathcal{K}}}$.

The proof of (b) ⇔ (d) and (c) ⇔ (e) is trivial, as $\mathrm{sat}_i(\mathcal{T}) = \mathrm{sat}(\mathcal{T}) \cap \mathcal{K}[\boldsymbol{u}][\boldsymbol{y}_i]$ and $\mathrm{sat}_i(\mathcal{T})_{\tilde{\mathcal{K}}} = \mathrm{sat}(\mathcal{T})_{\tilde{\mathcal{K}}} \cap \tilde{\mathcal{K}}[\boldsymbol{y}_i]$. □

Recall that a *perfect field* is one for which all algebraic extensions are separable. There is a simple criterion for perfectness: a field $\mathcal{K}$ is perfect if and only if

- $\mathcal{K}$ has characteristic 0, or
- $\mathcal{K}$ has characteristic $p > 0$ and every element of $\mathcal{K}$ has a pth root in $\mathcal{K}$.

For any $P \in \mathcal{K}[\boldsymbol{x}]$, we define the *separant* of P, denoted by $\mathrm{sep}(P)$, as the formal derivative of P w.r.t. its leading variable, i.e. $\mathrm{sep}(P) := \partial P/\partial\,\mathrm{lv}(P)$. For any triangular set $\mathcal{T}$ in $\mathcal{K}[\boldsymbol{x}]$, $\mathrm{sep}(\mathcal{T})$ denotes the set of separants of all the polynomials in $\mathcal{T}$.

Lemma 3.4. *Let $\mathcal{K}$ be a perfect field and $P \in \mathcal{K}[x]$. Then the following statements are equivalent.*

(a) *P is squarefree;*
(b) *P' is regular modulo $\langle P \rangle$.*

Proof. By [20, Theorem 7.36], we know that the squarefreeness of P is equivalent to $\gcd(P, P') = 1$, where P' is the derivative of P. Suppose that P is squarefree. Then $\gcd(P, P') = 1$, thus there exist $A, B \in \mathcal{K}[x]$ such that $AP + BP' = 1$. Therefore, in this case $BP' = 1$ modulo $\langle P\rangle$ and thus P' is regular modulo $\langle P\rangle$. If $\gcd(P, P') = G \in \mathcal{K}[x] \setminus \mathcal{K}$, then $P'(P/G) \in \langle P\rangle$ and $P/G \notin \langle P\rangle$; hence P' is not regular modulo $\langle P\rangle$. □

Proposition 3.5. *Let $\mathcal{T} = [T_1, \ldots, T_r]$ be a regular set in $\mathcal{K}[\boldsymbol{x}]$ and $\tilde{\mathcal{K}}$ be a perfect field. Then $\mathcal{T}$ is simple if and only if S is regular modulo $\mathrm{sat}(\mathcal{T})_{\tilde{\mathcal{K}}}$ for all $S \in \mathrm{sep}(\mathcal{T})$.*

Proof. ($\Rightarrow$) Suppose that $\mathcal{T}$ is a simple set and $S = \mathrm{sep}(T_i)$ is not regular modulo $\mathrm{sat}(\mathcal{T})_{\tilde{\mathcal{K}}}$ for some $i \in \{1, \ldots, r\}$. Then S is not regular modulo $\mathrm{sat}_i(\mathcal{T})_{\tilde{\mathcal{K}}}$. Hence there exists an $F \in \tilde{\mathcal{K}}[\boldsymbol{y}_i]$ such that $SF \in \mathrm{sat}_i(\mathcal{T})_{\tilde{\mathcal{K}}}$, but $F \notin \mathrm{sat}_i(\mathcal{T})_{\tilde{\mathcal{K}}}$. Thus by Lemma 3.2 there exists some associated prime $\mathfrak{p}$ of $\mathrm{sat}_{i-1}(\mathcal{T})_{\tilde{\mathcal{K}}}$ such that $\overline{F}^{\mathfrak{p}} \notin \overline{\mathrm{sat}_i(\mathcal{T})}^{\mathfrak{p}}_{\tilde{\mathcal{K}}}$, and by Lemma 3.1 we have $\overline{S}^{\mathfrak{p}}\overline{F}^{\mathfrak{p}} \in \overline{\mathrm{sat}_i(\mathcal{T})}^{\mathfrak{p}}_{\tilde{\mathcal{K}}} = \langle \overline{T}_i^{\mathfrak{p}}\rangle$. Therefore, $\overline{S}^{\mathfrak{p}}$ is not regular modulo $\langle \overline{T}_i^{\mathfrak{p}}\rangle$, and by Lemma 3.4, $\overline{T}_i^{\mathfrak{p}}$ is not squarefree. This leads to a contradiction, so every $S \in \mathrm{sep}(\mathcal{T})$ must be regular modulo $\mathrm{sat}(\mathcal{T})_{\tilde{\mathcal{K}}}$.

($\Leftarrow$) For any $T_i \in \mathcal{T}$, suppose that $S_i = \mathrm{sep}(T_i)$ is regular modulo $\mathrm{sat}(\mathcal{T})_{\tilde{\mathcal{K}}}$ and thus regular modulo $\mathrm{sat}_i(\mathcal{T})_{\tilde{\mathcal{K}}}$. Then for any associated prime $\mathfrak{p}$ of $\mathrm{sat}_{i-1}(\mathcal{T})_{\tilde{\mathcal{K}}}$, $\overline{S}_i^{\mathfrak{p}}$ is regular modulo $\langle \overline{T}_i^{\mathfrak{p}}\rangle$. By Lemma 3.4, $\overline{T}_i^{\mathfrak{p}}$ is squarefree. Consequently, $\mathcal{T}$ is simple. □

Let $\mathcal{T} \subseteq \mathcal{K}[\boldsymbol{x}]$ be a regular set and $S \in \mathcal{K}[\boldsymbol{x}]$; S can be regarded as an element in $\tilde{\mathcal{K}}[\boldsymbol{y}]$. It is easy to check that S is regular modulo $\mathrm{sat}(\mathcal{T})$ if and only if S is regular modulo $\mathrm{sat}(\mathcal{T})_{\tilde{\mathcal{K}}}$, as $\mathrm{sat}(\mathcal{T})_{\tilde{\mathcal{K}}} = (\mathcal{K}[\boldsymbol{u}] \setminus \{0\})^{-1}\mathrm{sat}(\mathcal{T})$.

Corollary 3.6. *Let $\mathcal{T}$ be a regular set in $\mathcal{K}[\boldsymbol{x}]$ and $\tilde{\mathcal{K}}$ be a perfect field. Then $\mathcal{T}$ is simple if and only if S is regular modulo $\mathrm{sat}(\mathcal{T})$ for all $S \in \mathrm{sep}(\mathcal{T})$.*

If the field $\tilde{\mathcal{K}}$ is not perfect, then the conclusions of Proposition 3.5 and Corollary 3.6 do not necessarily hold. For example, $[y^3 - u] \subseteq \mathbb{F}_3[u, y]$ is a simple set, but $\mathrm{sep}(y^3 - u) = 0$ (under $u < y$). As fields of characteristic 0 are perfect, the equivalent condition in Corollary 3.6 may be used to define simple sets over the field of rational numbers (see, e.g., [6]).

3.2. Ideal decomposition

Let $\mathcal{K}$ be an arbitrary field and $\mathcal{F}$ be any polynomial set in $\mathcal{K}[\boldsymbol{x}]$. An algorithm is presented in [10] to decompose $\mathcal{F}$ into a finite number of regular sets with an associated ideal relation. Similar algorithms can be found in [9,13,14,6]. For convenience of later use, we give a specification of the algorithm as follows.

Specification 1: Regular Decomposition $\mathbb{S} := \mathsf{RegDec}(\mathcal{F})$

Input: $\mathcal{F}$ — a polynomial set in $\mathcal{K}[\boldsymbol{x}]$, where $\mathcal{K}$ is an arbitrary field.
Output: $\mathbb{S}$ — a set of regular sets in $\mathcal{K}[\boldsymbol{x}]$ such that $\sqrt{\langle \mathcal{F}\rangle} = \bigcap_{\mathcal{T}\in\mathbb{S}} \sqrt{\mathrm{sat}(\mathcal{T})}$.

Now we review the pgcd algorithm, a generalization of standard gcd algorithms, as described in [6]. It is a key ingredient in relevant algorithms of regular sets. In what follows, we use $\mathcal{K}[\boldsymbol{x}][z]$ to denote the polynomial ring with all variables in $\boldsymbol{x}$ smaller than z. For any ring $\mathcal{R}$, the total quotient ring of $\mathcal{R}$, denoted by $\mathrm{fr}(\mathcal{R})$, is the localization of $\mathcal{R}$ at the multiplicatively closed set of all its elements that are not zero divisors.

Specification 2: Pseudo-gcd $\{(G_1, \mathcal{A}_1), \ldots, (G_s, \mathcal{A}_s)\} := \mathsf{pgcd}(\mathcal{F}, \mathcal{T})$

Input: $\mathcal{T}$ — a regular set in $\mathcal{K}[\boldsymbol{x}]$, where $\mathcal{K}$ is an arbitrary field;
$\mathcal{F}$ — a polynomial set in $\mathcal{K}[\boldsymbol{x}][z]$.
Output: $\{(G_1, \mathcal{A}_1), \ldots, (G_s, \mathcal{A}_s)\}$ — a set of pairs such that
(a) each $\mathcal{A}_i$ is a regular set in $\mathcal{K}[\boldsymbol{x}]$ and $\mathrm{sat}(\mathcal{T}) \subseteq \mathrm{sat}(\mathcal{A}_i)$;
(b) $\sqrt{\mathrm{sat}(\mathcal{T})} = \sqrt{\mathrm{sat}(\mathcal{A}_1)} \cap \cdots \cap \sqrt{\mathrm{sat}(\mathcal{A}_s)}$ is an irredundant decomposition;
(c) $\langle \mathcal{F}\rangle = \langle G_i\rangle$ in $\mathrm{fr}(\mathcal{K}[\boldsymbol{x}]/\mathrm{sat}(\mathcal{A}_i))[z]$;
(d) $G_i \in \langle \mathcal{F}\rangle + \mathrm{sat}(\mathcal{A}_i)$;
(e) $G_i = 0$, or $\mathrm{lc}(G_i, z)$ is regular modulo $\mathrm{sat}(\mathcal{A}_i)$.

In (b), "irredundant" means that the sets of associate primes of all $\mathrm{sat}(\mathcal{A}_i)$ give a partition of the set of associate primes of $\mathrm{sat}(\mathcal{T})$. More precisely, for any associated prime $\mathfrak{p}$ of $\mathrm{sat}(\mathcal{T})$, there exists a unique i such that $\sqrt{\mathrm{sat}(\mathcal{A}_i)} \subseteq \mathfrak{p}$.

The set $\{(G_1, \mathcal{A}_1), \ldots, (G_s, \mathcal{A}_s)\}$ satisfying the five conditions (a)–(e) above is called the *pseudo-gcd* of $\mathcal{F}$ w.r.t. $\mathcal{T}$. Similar algorithms are presented in [10,14], where the pseudo-gcd is called *generalized gcd* and *regular gcd* respectively.

Remark 3.1. In the specification of pgcd, now suppose that $\mathcal{T}$ is a simple set. Then $\mathrm{sat}(\mathcal{T})$ is radical by Theorem 3.3. We can show that $\mathrm{sat}(\mathcal{A}_i)$ is also radical for any $i = 1, \ldots, s$ as follows. Let $\mathfrak{q}$ be any primary component of $\mathrm{sat}(\mathcal{A}_i)$ and $\mathfrak{p} = \sqrt{\mathfrak{q}}$. One knows from (b) that $\mathfrak{p}$ is a prime component of $\mathrm{sat}(\mathcal{T})$. Let $\mathcal{S} = \mathcal{K}[\boldsymbol{x}] \setminus \mathfrak{p}$. It is easy to verify that $\mathcal{S}$ intersects with every

prime component of $\mathrm{sat}(\mathcal{T})$ other than $\mathfrak{p}$. By (a), $\mathrm{sat}(\mathcal{T}) \subseteq \mathrm{sat}(\mathcal{A}_i)$. Performing localization at $\mathcal{S}$ on this formula and then contracting back, we get $\mathfrak{p} \subseteq \mathfrak{q}$. Hence $\mathfrak{q} = \mathfrak{p}$, i.e. every primary component of $\mathrm{sat}(\mathcal{A}_i)$ is prime. Hence $\mathrm{sat}(\mathcal{A}_i)$ is radical. Again by Theorem 3.3, $\mathcal{A}_i$ is a simple set in $\mathcal{K}[\boldsymbol{x}]$. Furthermore, the ideal relation $\mathrm{sat}(\mathcal{T}) = \mathrm{sat}(\mathcal{A}_1) \cap \cdots \cap \mathrm{sat}(\mathcal{A}_s)$ is obtained.

Since $\mathrm{fr}(\mathcal{K}[\boldsymbol{x}]/\mathrm{sat}(\mathcal{A}_i)) = \tilde{\mathcal{K}}[\boldsymbol{y}]/\mathrm{sat}(\mathcal{A}_i)_{\tilde{\mathcal{K}}}$ as indicated in [6], by (c), $\langle \overline{\mathcal{F}}^{\mathfrak{p}} \rangle = \langle \overline{G}_i^{\mathfrak{p}} \rangle$ holds for any associated prime $\mathfrak{p}$ of $\mathrm{sat}(\mathcal{A}_i)_{\tilde{\mathcal{K}}}$. Hence $\overline{G}_i^{\mathfrak{p}}$ is equal to $\gcd(\overline{\mathcal{F}}^{\mathfrak{p}})$ in $(\tilde{\mathcal{K}}[\boldsymbol{y}]/\mathfrak{p})[z]$.

For decomposing a polynomial set into simple sets, there are two strategies. One is to integrate the squarefreeing process into regular decomposition as in [12], and the other is to first decompose the polynomial set into regular sets and then turn the obtained regular sets into simple sets. The specification of a turning algorithm presented in [6] for this latter strategy in the characteristic 0 case is given below.

Specification 3: Regular Sets to Simple Sets $\mathbb{S} := \mathsf{Reg2Sim}(\mathcal{T})$

Input: $\mathcal{T}$ — a regular set in $\mathcal{K}[\boldsymbol{x}]$, where $\mathcal{K}$ is a field of characteristic 0.
Output: $\mathbb{S}$ — a finite set of simple sets in $\mathcal{K}[\boldsymbol{x}]$ such that $\sqrt{\mathrm{sat}(\mathcal{T})} = \bigcap_{\mathcal{B}\in\mathbb{S}} \mathrm{sat}(\mathcal{B})$ is an irredundant decomposition.

From Remark 3.1 one knows that for any $(G_i, \mathcal{A}_i) \in \mathsf{pgcd}(\{F, \mathrm{sep}(F)\}, \mathcal{T})$ and associated prime $\mathfrak{p}$ of $\mathrm{sat}(\mathcal{A}_i)_{\tilde{\mathcal{K}}}$, $\overline{G_i}^{\mathfrak{p}} = \gcd(\overline{F}^{\mathfrak{p}}, \overline{\mathrm{sep}(F)}^{\mathfrak{p}})$. As a generalization from $P/\gcd(P, P')$ for the computation of the squarefree part of a univariate polynomial P, this property is used in Specification 3 to realize the conversion from regular sets to simple ones.

Combining Specifications 1 and 3, one can design an algorithm to decompose any polynomial set over a field $\mathcal{K}$ of characteristic 0 into simple sets. More precisely, given an $\mathcal{F} \subseteq \mathcal{K}[\boldsymbol{x}]$ as input, this algorithm returns a finite set $\mathbb{S}$ such that

- every $\mathcal{T} \in \mathbb{S}$ is a simple set;
- $\sqrt{\langle \mathcal{F} \rangle} = \bigcap_{\mathcal{T}\in\mathbb{S}} \mathrm{sat}(\mathcal{T})$.

Here $\mathbb{S}$ is called a *simple decomposition* of $\mathcal{F}$. By using this decomposition, radical ideal membership may be easily tested: for any $P \in \mathcal{K}[\boldsymbol{x}]$, $P \in \sqrt{\langle \mathcal{F} \rangle}$ if and only if $P \in \mathrm{sat}(\mathcal{T})$ for all $\mathcal{T} \in \mathbb{S}$, so by Proposition 2.2, one only needs to check whether or not $\mathrm{prem}(P, \mathcal{T}) \equiv 0$ for all $\mathcal{T} \in \mathbb{S}$.

4. Squarefree decomposition

We use $\mathbb{F}_q$ to denote the finite field of characteristic $p > 0$ with q elements. The algorithm for computing simple sets over any field $\mathcal{K}$ of characteristic 0 has been reviewed in the previous section, but it may fail when the field $\mathcal{K}$ is replaced by $\mathbb{F}_q$. The failure is caused by the use of $T/\gcd(T, T')$ in the algorithm for computing the squarefree part of a univariate polynomial T, for which some factors may be lost in the finite field case.

Consider for example $T = (x^3 - 2)(x - 1)^2 \in \mathbb{F}_3[x]$. Then

$$\mathrm{sep}(T) = 2(x^3 - 2)(x - 1) \quad \text{and} \quad T/\gcd(T, \mathrm{sep}(T)) = x - 1.$$

However, in $\mathbb{F}_3[x]$, $x^3 - 2 = (x - 2)^3$, so the squarefree part of T is actually $(x - 2)(x - 1)$. This example illustrates why we need to use additional techniques for computing the squarefree parts of polynomials over finite fields.

4.1. Squarefree decomposition of univariate polynomials over finite fields

First we recall the method of computing squarefree decompositions of univariate polynomials over finite fields from [21], which is the starting point for our later discussions. The reader may refer to the original paper for more details.

Let $F, A_i \in \mathcal{K}[x] \setminus \mathcal{K}$ and a_i be a positive integer for $i = 1, \ldots, s$. We call $\{[A_1, a_1], \ldots, [A_s, a_s]\}$ the *squarefree decomposition* and $A_1 \cdots A_s$ the *squarefree part* of F if the following conditions are satisfied:

- $F \sim A_1^{a_1} \cdots A_s^{a_s}$, which means that there exists a nonzero constant $b \in \mathcal{K}$ such that $F = b \cdot A_1^{a_1} \cdots A_s^{a_s}$;
- $\gcd(A_i, A_j) = 1$ for all $i \neq j$;
- A_i is squarefree for all $i = 1, \ldots, s$.

Proposition 4.1. *Let $\mathcal{K}$ be a field of characteristic $p > 0$. For any $F \in \mathcal{K}[x]$, there exist unique (up to unit) polynomials $P_1, \ldots, P_k$ and Q in $\mathcal{K}[x]$ such that*

(a) $F = Q \prod_{i=1}^{k} P_i^i$;
(b) $\gcd(P_i, P_i') = 1$, *which means that P_i is squarefree for all $i = 1, \ldots, k$;*
(c) $\gcd(P_i, P_j) = \gcd(P_i, Q) = 1$ *for all $i \neq j$;*

(d) $Q' = 0$;
(e) *if* $i \equiv 0 \bmod p$, *then* $P_i = 1$.

Corollary 4.2. *Let* $\mathcal{K}$ *be a field of characteristic* $p > 0$ *and* $F = Q\prod_{i=1}^{k} P_i^i$ *be the decomposition given in Proposition 4.1. Then* $\gcd(F, F') = Q\prod_{i=1}^{k} P_i^{i-1}$.

Proposition 4.3. *Let* $\mathcal{K}$ *be a field of characteristic* $p > 0$ *and* $F \in \mathcal{K}[x]$. *Then* $F' = 0$ *if and only if there exists a polynomial* $G \in \mathcal{K}[x]$ *such that* $F(x) = G(x^p)$.

For any $F \in \mathbb{F}_q[x] \setminus \mathbb{F}_q$, let $F = Q\prod_{i=1}^{k} P_i^i$ be the decomposition in Proposition 4.1. When $Q \in \mathbb{F}_q[x] \setminus \mathbb{F}_q$, the squarefree part of F is $Q_1\prod_{i=1}^{k} P_i$, where Q_1 is the squarefree part of Q. However, by Corollary 4.2,

$$\gcd(F, F') = Q\prod_{i=1}^{k} P_i^{i-1} \quad \text{and} \quad F/\gcd(F, F') = \prod_{i=1}^{k} P_i.$$

Hence using $F/\gcd(F, F')$ to obtain the squarefree part will cause Q_1 missing. This problem can be solved by the squarefree decomposition algorithm described below.

Algorithm 4: Squarefree Decomposition of a Univariate Polynomial $\mathbb{S} := \mathsf{sqf}(F)$

Input: F — a polynomial in $\mathbb{F}_q[x] \setminus \mathbb{F}_q$.
Output: $\mathbb{S}$ — the squarefree decomposition of F.

4.1 $\mathbb{S} := \emptyset$; $d := 1$;
4.2 $C_1 := \gcd(F, F')$;
4.3 $B_1 := F/C_1$;
4.4 **while** $B_1 \in \mathbb{F}_q[x] \setminus \mathbb{F}_q$ **do**
4.5 $\quad B_2 := \gcd(B_1, C_1)$;
4.6 $\quad C_2 := C_1/B_2$;
4.7 $\quad P := B_1/B_2$;
4.8 $\quad$ **if** $P \in \mathbb{F}_q[x] \setminus \mathbb{F}_q$ **then** $\mathbb{S} := \mathbb{S} \cup \{[P, d]\}$;
4.9 $\quad B_1 := B_2$; $C_1 := C_2$; $d := d + 1$;
4.10 **end**
4.11 **if** $C_1 \in \mathbb{F}_q[x] \setminus \mathbb{F}_q$ **then**
4.12 $\quad C_3 :=$ the pth root of C_1;
4.13 $\quad \{[A_1, a_1], \ldots, [A_s, a_s]\} := \mathsf{sqf}(C_3)$;
4.14 $\quad \mathbb{S} := \mathsf{merge}(\{[A_1, a_1 \cdot p], \ldots, [A_s, a_s \cdot p]\}, \mathbb{S})$;
4.15 **end**

In this and other algorithms, the operation $\mathsf{merge}(\{[A_1, a_1], \ldots, [A_s, a_s]\}, \{[D_1, d_1], \ldots, [D_t, d_t]\})$ first merges the two sets into one and then replaces any $[A_i, a_i]$ and $[D_j, d_j]$ for which $A_i = D_j$ by $[A_i, a_i + d_j]$.

Termination. Algorithm 4 is recursively called in line 4.13 when $C_1 \notin \mathbb{F}_q$. As C_3 in line 4.13 has smaller degree than F, we can assume that $\mathsf{sqf}(C_3)$ terminates by induction. So we only need to prove that the **while** loop terminates. This is obvious because $\deg(B_1)$ decreases strictly after each loop.

Correctness. Suppose that $F = Q\prod_{i=1}^{k} P_i^i$ is the decomposition in Proposition 4.1. Then we have $C_1 = QP_2P_3^2\cdots P_k^{k-1}$ in line 4.2 by Corollary 4.2 and thus $B_1 = P_1P_2\cdots P_k$ in line 4.3. Use $B_2(i), C_2(i), P(i)$ to denote B_2, C_2, P in the ith **while** loop respectively. It is easy to check that $B_2(i) = P_{i+1}\cdots P_k, C_2(i) = QP_{i+2}P_{i+3}^2\cdots P_k^{k-i-1}, P(i) = P_i$, and the **while** loop terminates when $C_1 \sim Q$. After the **while** loop is completed, if $C_1 \in \mathbb{F}_q$, then we have obtained the squarefree decomposition. Otherwise, the **if** block is performed to compute the squarefree decomposition of the pth root of C_1 recursively. The feasibility of the pth root extraction in line 4.12 is proved as follows. By Proposition 4.3, C_1 can be written in the form $C_1 = \sum_i a_i x^{ip}$, where $a_i \in \mathbb{F}_q$. Since $\mathbb{F}_q$ is a perfect field, the pth root b_i of each a_i exists. Hence the pth root of C_1 is $\sum_i b_i x^i$. After the algorithm terminates, one will obtain the complete squarefree decomposition of F.

4.2. Pseudo-squarefree decomposition

In this subsection, we generalize the squarefree decomposition algorithm presented above. Only the zero-dimensional case is considered here because positive-dimensional polynomial sets cannot be handled with our technique. More explanations will be given in the next subsection.

Definition 4.1. For any simple set $\mathcal{T} \subseteq \mathcal{K}[\boldsymbol{x}]$ and polynomial $F \in \mathcal{K}[\boldsymbol{x}][z] \setminus \mathcal{K}[\boldsymbol{x}]$, the *pseudo-squarefree decomposition* (or *generalized squarefree decomposition*) of F w.r.t. $\mathcal{T}$ is a set $\{(\{[A_{i1}, a_{i1}], \ldots, [A_{ik_i}, a_{ik_i}]\}, \mathcal{A}_i) : i = 1, \ldots, s\}$ such that

(a) $\mathcal{A}_i$ is a simple set in $\mathcal{K}[\boldsymbol{x}]$ for $i = 1, \ldots, s$;
(b) $\mathrm{sat}(\mathcal{T}) = \mathrm{sat}(\mathcal{A}_1) \cap \cdots \cap \mathrm{sat}(\mathcal{A}_s)$ is an irredundant decomposition;
(c) each $\{[\overline{A}_{i1}^{\mathfrak{p}}, a_{i1}], \ldots, [\overline{A}_{ik_i}^{\mathfrak{p}}, a_{ik_i}]\}$ is the squarefree decomposition of $\overline{F}^{\mathfrak{p}}$ for any associated prime $\mathfrak{p}$ of $\mathrm{sat}(\mathcal{A}_i)$.

Algorithm 5: Pseudo-squarefree Decomposition $\mathbb{S} := \mathsf{psqf}(F, \mathcal{T})$

Input: F — a polynomial in $\mathbb{F}_q[\boldsymbol{x}][z] \setminus \mathbb{F}_q[\boldsymbol{x}]$;
$\mathcal{T}$ — a zero-dimensional simple set in $\mathbb{F}_q[\boldsymbol{x}]$.
Output: $\mathbb{S}$ — the pseudo-squarefree decomposition of F w.r.t. $\mathcal{T}$.

```
5.1  S := ∅; D := ∅;
5.2  for (C1, C) ∈ pgcd({F, sep(F)}, T) do
5.3  |  B1 := pquo(F, C1);
5.4  |  D := D ∪ {[B1, C1, C, ∅, 1]};
5.5  end
5.6  while D ≠ ∅ do
5.7  |  [B1, C1, C, P, d] := pop(D);
5.8  |  if deg(B1, z) > 0 then
5.9  |  |  for (B2, A) ∈ pgcd({B1, C1}, C) do
5.10 |  |  |  C2 := pquo(C1, B2);
5.11 |  |  |  P := pquo(B1, B2);
5.12 |  |  |  if deg(P, z) > 0 then P := P ∪ {[P, d]};
5.13 |  |  |  D := D ∪ {[B2, C2, A, P, d + 1]};
5.14 |  |  end
5.15 |  else
5.16 |  |  if deg(C1, z) > 0 then
5.17 |  |  |  C3 := the pth root of C1 in (Fq[x]/sat(C))[z];
5.18 |  |  |  for ({[A1, a1], ..., [As, as]}, B) ∈ psqf(C3, C) do
5.19 |  |  |  |  S := S ∪ {(merge({[A1, a1 · p], ..., [As, as · p]}, P), B)};
5.20 |  |  |  end
5.21 |  |  else
5.22 |  |  |  S := S ∪ {(P, C)};
5.23 |  |  end
5.24 |  end
5.25 end
```

In this and other algorithms, the operation $\mathsf{pop}(\mathbb{D})$ means to take one element randomly and then delete it from $\mathbb{D}$. The above algorithm is a generalization of sqf. In this algorithm, $\mathbb{D}$ stores what to be processed. For each element $[B, C, \mathcal{C}, \mathbb{P}, d] \in \mathbb{D}$, $\mathcal{C}$ is a simple set over which later computation is to be performed; $\mathbb{P}$ stores the squarefree components already obtained, which are of power smaller than d.

Proof. Termination. Suppose that the call $\mathsf{psqf}(C, \mathcal{T})$ terminates for any polynomial C whose degree in z is smaller than $\deg(F, z)$ by induction. As the **while** loop is essentially a splitting procedure, we can regard it as building trees with elements in $\mathbb{D}$ as their nodes. The roots of these trees are built in lines 5.2–5.5. For each node $[B_1, C_1, \mathcal{C}, \mathbb{P}, d]$, its child $[B_2, C_2, \mathcal{A}, \mathbb{P}, d + 1]$ is constructed in line 5.13 with $\deg(B_2, z) < \deg(B_1, z)$ and the parameter d indicates its depth in the trees. Hence each path of the trees must be finite. The termination of line 5.18, where psqf is called recursively, follows from the induction hypothesis, as it is easy to see that the degree of C_3 in z is smaller than $\deg(F, z)$. Consequently, the **while** loop terminates, and the termination of the algorithm follows.

Correctness. The conditions (a) and (b) of Definition 4.1 follow from Remark 3.1 and the irredundant property of the ideal decomposition by pgcd.

For any fixed path of one of the trees, we denote the node of depth i in the path by $[B(i), C(i), \mathcal{C}(i), \mathbb{P}(i), i]$, where $i \leq s$, the length of the path. For any associated prime $\mathfrak{p}$ of $\mathrm{sat}(\mathcal{C}(s))$ in the leaf node, $\overline{F}^{\mathfrak{p}}$ is a univariate polynomial over the field $\mathbb{F}_q[\boldsymbol{x}]/\mathfrak{p}$. Thus we can assume that $\overline{F}^{\mathfrak{p}} = Q \prod_{i=1}^{s-1} P_i^i$ is the decomposition of $\overline{F}^{\mathfrak{p}}$ as in Proposition 4.1. By the properties of pgcd, it is easy to check that $\overline{B(i)}^{\mathfrak{p}} \sim P_i P_{i+1} \cdots P_{s-1}$ and $\overline{C(i)}^{\mathfrak{p}} \sim Q P_{i+1} P_{i+2}^2 \cdots P_{s-1}^{s-i-1}$. In particular, $\overline{B(s)}^{\mathfrak{p}} \sim 1$ and $\overline{C(s)}^{\mathfrak{p}} \sim Q$. Hence $C(s)$ can be written in the form $\sum_i c_i z^{pi}$, where $c_i \in \mathbb{F}_q[\boldsymbol{x}]/\mathrm{sat}(\mathcal{C}(s))$. In the next step, if $\deg(C_1, z) = 0$, then the squarefree decomposition of F is obtained. Otherwise, lines 5.17–5.20 are executed to compute C_3, the pth root of $C(s)$ (i.e. C_1), and then the squarefree decomposition of C_3. The extraction of pth roots of polynomials in $(\mathbb{F}_q[\boldsymbol{x}]/\mathrm{sat}(\mathcal{T}))[z]$, where $\mathcal{T}$ is a zero-dimensional simple set in $\mathbb{F}_q[\boldsymbol{x}]$, will be discussed in the next subsection. Hence condition (c) of Definition 4.1 follows clearly from the above analysis (analogous to the correctness proof of Algorithm 4). □

Let $(\{[A_1, a_1], \ldots, [A_s, a_s]\}, \mathcal{A})$ be an element of the output of Algorithm 5. Some A_i may not be reduced w.r.t. $\mathcal{A}$. To obtain simpler results, one can replace line 5.11 by "$P := \mathrm{prem}(\mathrm{pquo}(B_1, B_2), \mathcal{A})$;" and even do so for lines 5.3 and 5.10 in a similar way.

4.3. Extracting pth roots

Now we discuss the remaining issue in Algorithm 5: extracting the pth root of a polynomial $\sum_i c_i z^{pi} \in (\mathbb{F}_q[\boldsymbol{x}]/\mathrm{sat}(\mathcal{T}))[z]$, where $\mathcal{T}$ is a zero-dimensional simple set. This issue can be reduced to the extraction of the pth roots of the elements c_i in $\mathbb{F}_q[\boldsymbol{x}]/\mathrm{sat}(\mathcal{T})$. The following proposition exhibits the structure of $\mathbb{F}_q[\boldsymbol{x}]/\mathrm{sat}(\mathcal{T})$.

Proposition 4.4. *Let $\mathcal{T} = [T_1, \ldots, T_n]$ be a zero-dimensional simple set in $\mathbb{F}_q[\boldsymbol{x}]$. Then, for any $i = 1, \ldots, n$, $\mathbb{F}_q[\boldsymbol{x}_i]/\mathrm{sat}_i(\mathcal{T})$ is isomorphic to a product of perfect fields of characteristic $p > 0$. Furthermore, there exists a unique pth root for every element in $\mathbb{F}_q[\boldsymbol{x}_i]/\mathrm{sat}_i(\mathcal{T})$.*

Proof. For $i = 1$, by the Chinese remainder theorem, $\mathbb{F}_q[x_1]/\langle T_1\rangle$ is isomorphic to a product of fields, each of which is an algebraic extension of $\mathbb{F}_q$ and thus a perfect field. Suppose that the proposition is true for $i = k - 1$. We prove that it is also true for $i = k$ in the following. Let $\mathbb{F}_q[\boldsymbol{x}_{k-1}]/\mathrm{sat}_{k-1}(\mathcal{T}) \cong \mathcal{K}_1 \times \cdots \times \mathcal{K}_s$, where $\mathcal{K}_1, \ldots, \mathcal{K}_s$ are perfect fields, and $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ be the associated primes of $\mathrm{sat}_{k-1}(\mathcal{T})$ such that $\mathcal{K}_j = \mathbb{F}_q[\boldsymbol{x}_{k-1}]/\mathfrak{p}_j$. It is easy to show that $\mathbb{F}_q[\boldsymbol{x}_k]/\mathrm{sat}_k(\mathcal{T}) \cong \mathcal{K}_1[x_k]/\langle \overline{T}_k^{\mathfrak{p}_1}\rangle \times \cdots \times \mathcal{K}_s[x_k]/\langle \overline{T}_k^{\mathfrak{p}_s}\rangle$. For each $j = 1, \ldots, s$, $\mathcal{K}_j[x_k]/\langle \overline{T}_k^{\mathfrak{p}_j}\rangle$ is isomorphic to a product of fields, which are algebraic extensions of $\mathcal{K}_j$ and thus perfect. Consequently, $\mathbb{F}_q[\boldsymbol{x}_k]/\mathrm{sat}_k(\mathcal{T})$ is isomorphic to a product of perfect fields and the existence and uniqueness of the pth roots of its elements follow immediately. □

For a positive-dimensional simple set $\mathcal{T}$, $\tilde{\mathcal{F}}_q = \mathbb{F}_q(\boldsymbol{u})$ is not perfect, so the extraction of pth roots in $\tilde{\mathcal{F}}_q[\boldsymbol{y}_i]/\mathrm{sat}_i(\mathcal{T})_{\tilde{\mathcal{F}}_q}$ may be infeasible. Consider for example $\mathcal{T} = [y^3 - u] \subseteq \mathbb{F}_3[u, y]$. The 3rd root of u does not exist in $\mathbb{F}_3(u)[y]/\langle y^3 - u\rangle_{\mathbb{F}_3(u)}$. This explains why only the zero-dimensional case is addressed in this paper.

For any perfect field of characteristic $p > 0$, one can extract the pth roots of its elements by solving some linear equations (see, e.g., [21]). In view of the product structure of $\mathbb{F}_q[\boldsymbol{x}]/\mathrm{sat}(\mathcal{T})$, an obvious way for extracting the pth root of an element $F \in \mathbb{F}_q[\boldsymbol{x}]/\mathrm{sat}(\mathcal{T})$ is to compute the pth root of $\pi_j(F)$ over all the branches $\mathbb{F}_q[\boldsymbol{x}]/\mathfrak{p}_j$ and then lift them back, where $\mathfrak{p}_j$ $(j = 1, \ldots, s)$ are the associated primes of $\mathrm{sat}(\mathcal{T})$. The drawback of this method is that it needs to split the field product $\mathbb{F}_q[\boldsymbol{x}]/\mathrm{sat}(\mathcal{T})$ completely. As prime decomposition of $\mathrm{sat}(\mathcal{T})$ may involve the computation of Gröbner bases or irreducible triangular sets, one can imagine the ineffectiveness of this method.

In what follows, we propose another method for pth root extraction. The following two propositions serve as the basis of our method.

Proposition 4.5. *Let $\mathcal{T} = [T_1, \ldots, T_r] \subseteq \mathcal{K}[\boldsymbol{x}]$ be a simple set. Then, for any $i = 1, \ldots, r$, $\tilde{\mathcal{K}}[\boldsymbol{y}_i]/\mathrm{sat}_i(\mathcal{T})_{\tilde{\mathcal{K}}}$ is a $(\tilde{\mathcal{K}}[\boldsymbol{y}_{i-1}]/\mathrm{sat}_{i-1}(\mathcal{T})_{\tilde{\mathcal{K}}})$-module and $1, y_i, \ldots, y_i^{d-1}$ form a free basis (of this module), where $d = \deg(T_i, y_i)$.*

Proof. First we have

$$\tilde{\mathcal{K}}[\boldsymbol{y}_i]/\mathrm{sat}_i(\mathcal{T})_{\tilde{\mathcal{K}}} \cong (\tilde{\mathcal{K}}[\boldsymbol{y}_i]/\mathrm{sat}_{i-1}(\mathcal{T})_{\tilde{\mathcal{K}}})/(\mathrm{sat}_i(\mathcal{T})_{\tilde{\mathcal{K}}}/\mathrm{sat}_{i-1}(\mathcal{T})_{\tilde{\mathcal{K}}}).$$

Furthermore, $\tilde{\mathcal{K}}[\boldsymbol{y}_i]/\mathrm{sat}_{i-1}(\mathcal{T})_{\tilde{\mathcal{K}}} = (\tilde{\mathcal{K}}[\boldsymbol{y}_{i-1}]/\mathrm{sat}_{i-1}(\mathcal{T})_{\tilde{\mathcal{K}}})[y_i]$ and $\mathrm{sat}_i(\mathcal{T})_{\tilde{\mathcal{K}}}/\mathrm{sat}_{i-1}(\mathcal{T})_{\tilde{\mathcal{K}}} = \langle \overline{T}_i\rangle$, which is an ideal in $(\tilde{\mathcal{K}}[\boldsymbol{y}_{i-1}]/\mathrm{sat}_{i-1}(\mathcal{T})_{\tilde{\mathcal{K}}})[y_i]$. It follows that $\tilde{\mathcal{K}}[\boldsymbol{y}_i]/\mathrm{sat}_i(\mathcal{T})_{\tilde{\mathcal{K}}}$ is a $(\tilde{\mathcal{K}}[\boldsymbol{y}_{i-1}]/\mathrm{sat}_{i-1}(\mathcal{T})_{\tilde{\mathcal{K}}})$-module. Let $\overline{F} \in (\tilde{\mathcal{K}}[\boldsymbol{y}_{i-1}]/\mathrm{sat}_{i-1}(\mathcal{T})_{\tilde{\mathcal{K}}})[y_i]$. Since $\mathrm{lc}(\overline{T}_i)$ is regular and thus invertible in $\tilde{\mathcal{K}}[\boldsymbol{y}_{i-1}]/\mathrm{sat}_{i-1}(\mathcal{T})_{\tilde{\mathcal{K}}}$, we can divide $\overline{F}$ by $\overline{T}_i$. The remainder is a linear combination of $1, y_i, \ldots, y_i^{d-1}$, which is equal to $\overline{F}$ in $\tilde{\mathcal{K}}[\boldsymbol{y}_i]/\mathrm{sat}_i(\mathcal{T})_{\tilde{\mathcal{K}}}$. It is easy to verify the linear independence of $1, y_i, \ldots, y_i^{d-1}$. □

The elements $1, y_i, \ldots, y_i^{d-1}$ in the above proposition are called the *standard basis* of $\tilde{\mathcal{K}}[\boldsymbol{y}_i]/\mathrm{sat}_i(\mathcal{T})_{\tilde{\mathcal{K}}}$.

Proposition 4.6. *Let $\mathcal{R}$ be a ring isomorphic to a product of fields, M be an $n \times n$ matrix over $\mathcal{R}$, and $\boldsymbol{b} \in \mathcal{R}^n$. Then the set of linear equations*

$$M\boldsymbol{x} = \boldsymbol{b} \tag{2}$$

has a unique solution if and only if $\det(M)$ is regular in $\mathcal{R}$. If the equivalent conditions are satisfied, then the unique solution is $\boldsymbol{a} = (a_1, \ldots, a_s)$, where $a_i = \det(M_i) \cdot \det(M)^{-1}$ and M_i is the matrix obtained by replacing the ith column of M with $\boldsymbol{b}$.

Proof. Suppose that $\mathcal{R} \cong \mathcal{K}_1 \times \cdots \times \mathcal{K}_s$, where $\mathcal{K}_i$ is a field for $i = 1, \ldots, s$. We use π_i to denote the projection of $\mathcal{R}$ to $\mathcal{K}_i$. It induces two maps respectively from matrices and vectors over $\mathcal{R}$ to those over $\mathcal{K}_i$, which are also denoted by π_i. If $\boldsymbol{a} = (a_1, \ldots, a_n)$ is a solution of (2), then the following sets of equations may be obtained by projection:

$$\pi_i(M)\pi_i(\boldsymbol{a}) = \pi_i(\boldsymbol{b}), \quad i = 1, \ldots, s. \tag{3}$$

Thus solving (2) for $\boldsymbol{x}$ is equivalent to finding $\pi_i(\boldsymbol{a})$ satisfying (3) for all $i = 1, \ldots, s$. According to the Cramer's rule, each set of equations in (3) has a unique solution if and only if $\det(\pi_i(M)) = \pi_i(\det(M)) \neq 0$; if the equivalent conditions are satisfied, then $\pi_i(a_j) = \det(\pi_i(M_j)) \cdot \det(\pi_i(M))^{-1} = \pi_i(\det(M_j) \cdot \det(M)^{-1})$, where M_i is the matrix obtained by replacing the ith column of M with $\boldsymbol{b}$.

Hence (2) has a unique solution if and only if $\det(M)$ is regular in $\mathcal{R}$. If the equivalent conditions are satisfied, then one can find the unique solution $\boldsymbol{a} = (a_1, \ldots, a_s)$ with $a_i = \det(M_i) \cdot \det(M)^{-1}$. □

In the following, the simple set $\mathcal{T} = [T_1, \ldots, T_n] \subseteq \mathbb{F}_q[\boldsymbol{x}]$ is restricted to be zero-dimensional. Let $F \in \mathbb{F}_q[\boldsymbol{x}]$, $\mathrm{lv}(F) = x_i$, and $\deg(T_i, x_i) = d$. We want to construct a polynomial $G = a_0 + a_1 x_i + \cdots + a_{d-1} x_i^{d-1}$ with $a_j \in \mathbb{F}_q[\boldsymbol{x}_{i-1}]$ such that $G^p = F$ modulo $\mathrm{sat}_i(\mathcal{T})$.

Suppose that the pseudo-division formula of $G^p - F$ w.r.t. T_i is $C(G^p - F) = QT_i + R$, where C is some power of $\mathrm{ini}(T_i)$ and $R = \mathrm{prem}(G^p - F, T_i)$. The pseudo-remainder R can be written as $R = (f_{d-1} x_i^{d-1} + \cdots + f_0) + (b_{d-1} x_i^{d-1} + \cdots + b_0)$, where each f_j is a linear combination of $a_0^p, \ldots, a_{d-1}^p$ with coefficient in $\mathbb{F}_q[\boldsymbol{x}_{i-1}]$ and each b_j is an element in $\mathbb{F}_q[\boldsymbol{x}_{i-1}]$ for $j = 0, \ldots, d-1$. Noting that C is regular modulo $\mathrm{sat}_i(\mathcal{T})$, one can prove that $G^p = F$ modulo $\mathrm{sat}_i(\mathcal{T})$ is equivalent to

$$f_{d-1} x_i^{d-1} + \cdots + f_0 = -(b_{d-1} x_i^{d-1} + \cdots + b_0) \text{ modulo } \mathrm{sat}_i(\mathcal{T}).$$

Comparing the coefficients of x_i^j $(j = 0, \ldots, d-1)$ in this equality, we obtain the following set of equations modulo $\mathrm{sat}_{i-1}(\mathcal{T})$:

$$\begin{aligned} &f_0(a_0^p, \ldots, a_{d-1}^p) = -b_0, \\ &f_1(a_0^p, \ldots, a_{d-1}^p) = -b_1, \\ &\vdots \\ &f_{d-1}(a_0^p, \ldots, a_{d-1}^p) = -b_{d-1}. \end{aligned} \tag{4}$$

As the existence and uniqueness of the pth roots of elements in $\mathbb{F}_q[\boldsymbol{x}_i]/\mathrm{sat}_i(\mathcal{T})$ have been proven, the set of linear equations (4) has a unique solution; hence we are able to solve it for $a_0^p, \ldots, a_{d-1}^p$ by Proposition 4.6. After a_j^p is obtained, we are in the position to compute the pth root a_j of a_j^p in $\mathbb{F}_q[\boldsymbol{x}_{i-1}]/\mathrm{sat}_{i-1}(\mathcal{T})$ for $j = 0, \ldots, d-1$. Repeating the above process will lead to pth root extraction in $\mathbb{F}_q$ in the end, which is computable. It should be noted that when using Proposition 4.6 to solve (4), one needs to obtain the inverse of an element in $\mathbb{F}_q[\boldsymbol{x}_{i-1}]/\mathrm{sat}_{i-1}(\mathcal{T})$, which can be computed by the algorithm QuasiRecip described in [22].

The whole process is illustrated by the following example.

Example 4.1. Consider the simple set $\mathcal{T} = [T_1, T_2] = [x^2 + 2x + 2, xy^2 + y + 1] \subseteq \mathbb{F}_5[x, y]$. We want to compute the 5th root of $F = y + 4x$ in $\mathbb{F}_5[x, y]/\mathrm{sat}(\mathcal{T})$. Suppose that $G = a_1 y + a_0$ is the 5th root of F. One has the pseudo-division formula of $G^5 - F$ w.r.t. T_2:

$$x^4(G^5 - F) = \mathrm{pquo}(G^5, T_2) \cdot T_2 + (x^2 a_1^5 + 2x a_1^5 + a_1^5)y + (x^4 a_0^5 + 3x a_1^5 + a_1^5) - (x^4 y + 4x^5).$$

Thus in $\mathbb{F}_5[x, y]/\mathrm{sat}(\mathcal{T})$, we have $(x^2 a_1^5 + 2x a_1^5 + a_1^5)y + (x^4 a_0^5 + 3x a_1^5 + a_1^5) - (x^4 y + 4x^5) = 0$. Equating the coefficients of y^i $(i = 1, 0)$ to 0, we obtain a set of linear equations in the matrix form

$$\begin{bmatrix} x^4 & 3x + 1 \\ 0 & x^2 + 2x + 1 \end{bmatrix} \begin{bmatrix} a_0^5 \\ a_1^5 \end{bmatrix} = \begin{bmatrix} 4x^5 \\ x^4 \end{bmatrix}. \tag{5}$$

Denote by M the coefficient matrix of (5) and by M_i the matrix obtained by replacing the $(i+1)$th column of M with $\begin{bmatrix} 4x^5 & x^4 \end{bmatrix}^T$ for $i = 0, 1$. By Proposition 4.6, $a_i^5 = \det(M_i) \cdot \det(M)^{-1}$ is the solution of (5). Using the algorithm QuasiRecip in [22], we find that the inverse of $\det(M) = x^4 (x^2 + 2x + 1)$ is 4. Hence the solution of (5) is $a_0^5 = x^7 + 2x^6 + 4x^5 + x^4$ and $a_1^5 = 4x^8$. Recursively extracting the 5th root of a_0^5 and a_1^5 in the same way, we get $G = 4y + 2x + 1$ in the end.

5. Computing simple sets over finite fields

A polynomial set $\mathcal{F}$ is said to be *zero-dimensional* if the ideal generated by the polynomials in $\mathcal{F}$ is zero-dimensional. In this section, we present algorithms to decompose zero-dimensional polynomial sets into simple sets over finite fields.

5.1. Ideal decomposition

Let $\mathcal{F}$ be a zero-dimensional polynomial set in $\mathbb{F}_q[\boldsymbol{x}]$. The following algorithm computes a finite number of simple sets $\mathcal{T}_1, \ldots, \mathcal{T}_r$ such that $\sqrt{\langle \mathcal{F} \rangle} = \bigcap_{i=1}^{r} \langle \mathcal{T}_i \rangle$.

Algorithm 6: Weak Simple Decomposition $\mathbb{S} := \mathsf{WSimDec}(\mathcal{F})$

Input: $\mathcal{F}$ — a zero-dimensional polynomial set in $\mathbb{F}_q[\boldsymbol{x}]$.
Output: $\mathbb{S}$ — a finite set of simple sets in $\mathbb{F}_q[\boldsymbol{x}]$ such that $\sqrt{\langle\mathcal{F}\rangle} = \bigcap_{\mathcal{B}\in\mathbb{S}}\langle\mathcal{B}\rangle$.

```
6.1  S := ∅;
6.2  for T ∈ RegDec(F) do
6.3  |  D := {(T, ∅)}; S_T := ∅;
6.4  |  while D ≠ ∅ do
6.5  |  |  (A, B) := pop(D);
6.6  |  |  if A = ∅ then
6.7  |  |  |  S_T := S_T ∪ {B};
6.8  |  |  else
6.9  |  |  |  A := the polynomial in A with smallest leading variable;
6.10 |  |  |  for ({[C_1, c_1], ..., [C_s, c_s]}, Q) ∈ psqf(A, B) do
6.11 |  |  |  |  D := D ∪ {(A \ {A}, Q ∪ {C_1 ··· C_s})};
6.12 |  |  |  end
6.13 |  |  end
6.14 |  end
6.15 |  S := S ∪ S_T;
6.16 end
```

Proof. It is easy to verify the termination of the algorithm. We prove the correctness as follows.

For any zero-dimensional regular set $\mathcal{T}$, $\mathrm{sat}(\mathcal{T}) = \langle\mathcal{T}\rangle$. By Specification 1, $\sqrt{\langle\mathcal{F}\rangle} = \bigcap_{\mathcal{T}\in\mathsf{RegDec}(\mathcal{F})}\sqrt{\langle\mathcal{T}\rangle}$. By Algorithm 5, one can easily verify that for any $(\mathcal{A}, \mathcal{B}) \in \mathbb{D}$, $\mathcal{B}$ is a simple set. Hence each element in $\mathbb{S}$ is a simple set.

To prove the ideal relation $\sqrt{\langle\mathcal{F}\rangle} = \bigcap_{\mathcal{B}\in\mathbb{S}}\langle\mathcal{B}\rangle$, we only need to prove that for each $\mathcal{T} \in \mathsf{RegDec}(\mathcal{F})$, $\sqrt{\langle\mathcal{T}\rangle} = \bigcap_{\mathcal{B}\in\mathbb{S}_\mathcal{T}}\langle\mathcal{B}\rangle$ holds at the end of the corresponding **while** loop for $\mathcal{T}$. For lines 6.10–6.12, the ideal relation

$$\sqrt{\langle\mathcal{A}\rangle + \langle\mathcal{B}\rangle} = \bigcap_{(\{[C_1,c_1],\ldots,[C_s,c_s]\},\mathcal{Q})\in\mathsf{psqf}(A,\mathcal{B})} \sqrt{\langle\mathcal{A}\rangle + \langle\mathcal{Q}\rangle}$$

holds. For each $(\{[C_1, c_1], \ldots, [C_s, c_s]\}, \mathcal{Q}) \in \mathsf{psqf}(A, \mathcal{B})$, we have

$$\sqrt{\langle\mathcal{A}\rangle + \langle\mathcal{Q}\rangle} = \sqrt{\langle\mathcal{A}\setminus\{A\}\rangle + \langle\mathcal{Q}\cup\{A\}\rangle} = \sqrt{\langle\mathcal{A}\setminus\{A\}\rangle + \sqrt{\langle\mathcal{Q}\cup\{A\}\rangle}} = \sqrt{\langle\mathcal{A}\setminus\{A\}\rangle + \langle\mathcal{Q}\cup\{C_1\cdots C_s\}\rangle}.$$

Hence the following invariant of the corresponding **while** loop for $\mathcal{T}$ follows:

$$\sqrt{\langle\mathcal{T}\rangle} = \bigcap_{(\mathcal{A},\mathcal{B})\in\mathbb{D}} \sqrt{\langle\mathcal{B}\cup\mathcal{A}\rangle} \cap \bigcap_{\mathcal{B}\in\mathbb{S}_\mathcal{T}} \langle\mathcal{B}\rangle. \quad \square$$

Next we discuss some variants of the algorithm WSimDec. Prejudging criteria are presented for excluding some cases in which complete squarefree decomposition is unnecessary.

We start with the univariate case. By Proposition 4.1, a polynomial $F \in \mathbb{F}_q[x]$ can be written in the form $F = Q\prod_i P_i^i$ with $Q' = 0$. If Q is a constant, then the squarefree part of Q can be obtained just by computing $F/\gcd(F, F')$; otherwise, we need squarefree decomposition as done in Algorithm 4. In other words, squarefree decomposition in the cases when Q is a constant may be avoided by identifying such cases. The key observation is as follows.

If Q is not a constant, then Q is a pth power of some nonconstant polynomial. In this case, the following conditions must be satisfied:

- $\deg(F) \geq p$;
- if $F^{(s)}$ is the last nonzero polynomial in the derivative sequence $F, F', F^{(2)}, \ldots, F^{(s)}, 0, \ldots,$ then $p|\deg(F^{(s)})$.

Let $\mathcal{T}$ be a simple set in $\mathbb{F}_q[\boldsymbol{x}]$ and $F \in \mathbb{F}_q[\boldsymbol{x}][z]$. These conditions can be generalized to the case of pseudo-squarefree decomposition:

- $\deg(F, z) \geq p$;
- if $\partial^s F/\partial z^s$ is the last regular polynomial modulo $\mathrm{sat}(\mathcal{T})$ in the derivative sequence $F, \partial F/\partial z, \partial^2 F/\partial z^2, \ldots, \partial^s F/\partial z^s, \ldots,$ then $p|\deg(\partial^s F/\partial z^s, z)$.

The above conditions can be used as criteria for identifying some cases in which the technique for computing the squarefree part in Specification 3 still works. However, for the second condition it is necessary to determine whether a polynomial is regular, which may be quite time-consuming as shown in Section 6. The modified version of WSimDec with the prejudging criteria incorporated is named as WSimDecPJ.

What we have actually computed is the complete squarefree decomposition, while only the squarefree part is needed. One can choose to split the squarefree part into factors. The splitting may lead to more branches, but polynomials in each

branch are simpler. We call the new algorithm with this splitting strategy the *strong simple decomposition algorithm*, denoted as SSimDec, which can be easily obtained by replacing line 6.11 of Algorithm 6 with the following statement

"$\mathbb{D} := \mathbb{D} \cup \{(\mathcal{A} \setminus \{A\}, \mathcal{Q} \cup \{C_i\}) : \ i = 1, \ldots, s\}$; ".

The output of SSimDec has the same properties as that of WSimDec, and the proof of termination and correctness is similar.

For instance, consider the regular set $\mathcal{T} = [(x+1)^4(x^3+2x+1), y^3+x+2]$ in the polynomial ring $\mathbb{F}_3[x, y]$ with $x < y$. SSimDec($\mathcal{T}$) yields two simple sets $[x+1, y+1]$ and $[x^3+2x+1, y+x]$, while WSimDec($\mathcal{T}$) returns $[x^4+x^3+2x^2+1, y+2x^3+2x+2]$.

The following example illustrates the entire process of our main algorithms.

Example 5.1. Consider the polynomial set $\mathcal{F} = \{F_1, F_2\} \subseteq \mathbb{F}_3[x, y]$, where

$$F_1 = (y^2+y+2x^2+2)(2xy+y+2x^2+2)(x^6y^6+2x^9y^3+2x^3y^3+x^{12}+2x^6+1),$$
$$F_2 = 2y^6+y^3+2x^6+1.$$

Order the variables as $x < y$. By the algorithm RegDec, $\mathcal{F}$ is decomposed into four regular sets

$$\mathcal{T}_1 = [x+1, y+2], \qquad \mathcal{T}_2 = [x+2, y+2], \qquad \mathcal{T}_3 = [x^2+1, y+1], \qquad \mathcal{T}_4 = [T_1, T_2],$$

where

$$T_1 = x^3+2x+1, \qquad T_2 = (x^2+2)y^4+(x^2+2x)y^3+(2x^2+x+1)y+x^2+2.$$

It is easy to check that $\mathcal{T}_1, \mathcal{T}_2, \mathcal{T}_3$ are all simple sets, but $\mathcal{T}_4$ is not. Thus further computation is needed to turn $\mathcal{T}_4$ into simple sets. In WSimDec, $\mathcal{T}_4$ is converted to

$$\mathcal{T}_4' = [T_1, (x^4+x^2+x)y^2+(2x^4+2x^3+2x^2+2)y+2x^3+2x+2],$$

which is a simple set. The output of WSimDecPJ is the same. To illustrate the prejudging criteria in WSimDecPJ, first consider T_1. Note that $\deg(T_1, x) = 3$ and the derivative sequence of T_1 is $T_1, 2, 0$. Thus the second prejudging criterion ensures that complete squarefree decomposition of T_1 is unnecessary and one can use $\gcd(T_1, T_1')/T_1$ only to obtain the squarefree part of T_1. For T_2, $\deg(T_2, y) > 3$ and its derivative sequence $T_2, 2y^3+x^2y^2+2x^2+x+1, 0$ satisfies the second prejudging criterion. Hence squarefree decomposition is still needed.

The algorithm SSimDec produces a finer decomposition, turning $\mathcal{T}_4$ into two simple sets

$$\mathcal{T}_{41} = [T_1, (x^2+x+2)y+x+2], \qquad \mathcal{T}_{42} = [T_1, (x^2+2x)y+2x^2+2x+1].$$

Consequently, two kinds of simple decomposition of $\mathcal{F}$ are obtained such that

$$\sqrt{\langle \mathcal{F} \rangle} = \bigcap_{i=1}^{3} \langle \mathcal{T}_i \rangle \cap \langle \mathcal{T}_4' \rangle = \bigcap_{i=1}^{3} \langle \mathcal{T}_i \rangle \cap \langle \mathcal{T}_{41} \rangle \cap \langle \mathcal{T}_{42} \rangle.$$

5.2. Zero decomposition

Let $\overline{\mathbb{F}}_q$ be the algebraic closure of $\mathbb{F}_q$. For any polynomial set $\mathcal{F} \subseteq \mathbb{F}_q[\boldsymbol{x}]$, denote the set of all common zeroes of $\mathcal{F}$ in $\overline{\mathbb{F}}_q^n$ by $\mathrm{Zero}(\mathcal{F})$. Now suppose that $\mathcal{F}$ is zero-dimensional. The ideal relation $\sqrt{\langle \mathcal{F} \rangle} = \bigcap_{\mathcal{B} \in \mathbb{S}} \langle \mathcal{B} \rangle$ is associated to all the simple decomposition algorithms with input $\mathcal{F}$ and output $\mathbb{S}$ described above. Thus we have the following zero decomposition in $\overline{\mathbb{F}}_q^n$:

$$\mathrm{Zero}(\mathcal{F}) = \bigcup_{\mathcal{B} \in \mathbb{S}} \mathrm{Zero}(\mathcal{B}).$$

In practice, zeroes in the ground field $\mathbb{F}_q$ are often of interest. For any polynomial set $\mathcal{F} \subseteq \mathbb{F}_q[\boldsymbol{x}]$, denote the set of zeroes of $\mathcal{F}$ in $\mathbb{F}_q^n$ by $\mathrm{Zero}_q(\mathcal{F})$.

Lemma 5.1. *Let T be any polynomial in $\mathbb{F}_q[x]$. Then $\tilde{T} = \gcd(T, x^q - x)$ is squarefree and* $\mathrm{Zero}_q(\{T\}) = \mathrm{Zero}(\{\tilde{T}\})$.

Proof. As the field equation $x^q - x = \prod_{\alpha \in \mathbb{F}_q} (x - \alpha)$ is squarefree and its roots cover $\mathbb{F}_q$, it is easy to verify that $\tilde{T}$ is squarefree and it keeps all the zeroes of T in $\mathbb{F}_q$. □

The above lemma makes it easy to compute a simple decomposition with an associated zero relation in the ground field. It is natural to design the following algorithm, which applies to arbitrary polynomial set $\mathcal{F} \subseteq \mathbb{F}_q[\boldsymbol{x}]$, zero-dimensional or not.

Algorithm 7: $\mathbb{S} := \mathsf{GSimDec}(\mathcal{F})$

Input: $\mathcal{F}$ — a polynomial set in $\mathbb{F}_q[\boldsymbol{x}]$.
Output: $\mathbb{S}$ — a finite set of simple sets in $\mathbb{F}_q[\boldsymbol{x}]$ such that $\mathrm{Zero}_q(\mathcal{F}) = \bigcup_{\mathcal{B}\in\mathbb{S}} \mathrm{Zero}(\mathcal{B})$.

```
7.1  S := ∅;
7.2  for T ∈ RegDec(F ∪ {x_1^q − x_1, ..., x_n^q − x_n}) do
7.3      D := {(T, ∅)}; S_T := ∅;
7.4      while D ≠ ∅ do
7.5          (A, B) := pop(D);
7.6          if A = ∅ then
7.7              S_T := S_T ∪ {B};
7.8          else
7.9              x_i := the smallest dependent of A;
7.10             A := the polynomial in A with leading variable x_i;
7.11             for (F, Q) ∈ pgcd({A, x_i^q − x_i}, B) do
7.12                 if deg(F, x_i) > 0 then D := D ∪ {(A \ {A}, Q ∪ {F})};
7.13             end
7.14         end
7.15     end
7.16     S := S ∪ S_T;
7.17 end
```

Proof. It is easy to verify the termination. Obviously,

$$\mathrm{Zero}_q(\mathcal{F}) = \mathrm{Zero}(\mathcal{F} \cup \{x_1^q - x_1, \ldots, x_n^q - x_n\}) = \bigcup_{\mathcal{T}\in\mathsf{RegDec}(\mathcal{F})} \mathrm{Zero}(\mathcal{T}).$$

The simpleness property of $\mathcal{B}$ is guaranteed by Lemma 5.1, and the following invariant of the corresponding **while** loop for $\mathcal{T}$ follows from the properties of pgcd:

$$\mathrm{Zero}(\mathcal{T}) = \bigcup_{(\mathcal{A},\mathcal{B})\in\mathbb{D}} \mathrm{Zero}(\mathcal{B} \cup \mathcal{A}) \cup \bigcup_{\mathcal{B}\in\mathbb{S}_\mathcal{T}} \mathrm{Zero}(\mathcal{B}). \quad \square$$

In the process of this algorithm, especially in RegDec, for any $i = 1, \ldots, n$, one can recursively replace every variable product x_i^d ($d \geq q$) effectively appearing in the intermediate polynomials other than the field equations by x_i^{d-q+1} until its power is smaller than q. This will not change the zero relation in $\mathbb{F}_q$ and is a typical technique to control the degree of intermediate polynomials. By using this technique the algorithm's efficiency may be improved, especially when the input polynomials have high degrees.

This algorithm can be divided into two steps: computing the regular decomposition of $\mathcal{F} \cup \{x_1^q - x_1, \ldots, x_n^q - x_n\}$, and then applying Lemma 5.1 to ensure that output regular sets are simple. According to our observation, the first step takes most of the execution time and yields regular sets which are already simple in most cases. Let $\mathcal{T} = [T_1, \ldots, T_n]$ be a regular set returned by the first step. If $\mathcal{T}$ is simple, then the second step is essentially to verify that each T_i divides $x_i^q - x_i$ for all $i = 1, \ldots, n$, which would not take much time. The following example illustrates this algorithm.

Example 5.2. Consider the polynomial set $\mathcal{F} = \{F_1, F_2\} \subseteq \mathbb{F}_3[x, y, z]$, where $F_1 = (x-1)^2(x-2)(x^2+1)$ and $F_2 = z^2 - y$. Order the variables as $x < y < z$. In the first step, $\mathsf{RegDec}(\mathcal{F} \cup \{x^3 - x, y^3 - y, z^3 - z\})$ may yield

$$\{[x+1, y, z], [x+1, y+2, z+1], [x+1, y+2, z+2], [x+2, y, z], [x+2, y+2, z+1], [x+2, y+2, z+2]\}.$$

These are already simple sets and further computation is just to verify that the polynomials in these simple sets divide the corresponding field equations.

To study zero decomposition in the ground field $\mathbb{F}_q$, one can also consider triangular decomposition of polynomial sets in the quotient ring $\mathcal{K}[\boldsymbol{x}]/\langle x_i^q - x_i : i = 1, \ldots, n\rangle$. The interested reader may consult [23,24].

6. Implementation and experiments

We have implemented the algorithms SSimDec, WSimDec, and WSimDecPJ in Maple using the RegularChains library [25]. As currently this library can only handle polynomial sets over prime finite fields, i.e. $\mathbb{F}_p$, our implementation also has this restriction. The regular decomposition algorithm RegDec used in Algorithm 5 has been implemented in the library, so we are only interested in the performance of simple decomposition from given regular sets and all our experiments were conducted for understanding this performance.

Table 1
Timings of decomposing regular sets into simple sets (in seconds).

No.	SSimDec	WSimDec	WSimDecPJ	Prejudge
P1	0.766 (21)	189.984 (16)	191.610 (16)	2.985
P2	331.750 (28)	392.437 (20)	163.891 (20)	16.094
P3	72.578 (72)	97.922 (36)	43.610 (36)	0.202
P4	18.922 (36)	16.907 (18)	11.687 (18)	7.890
P5	85.625 (24)	133.188 (12)	133.906 (12)	1.421
P6	96.187 (36)	187.047 (36)	76.641 (36)	8.641
P7	59.547 (108)	542.672 (180)	166.250 (180)	0.000
P8	924.687 (8)	653.297 (6)	382.391 (6)	0.000
P9	286.860 (4)	387.453 (2)	173.984 (2)	0.000
P10	80.812 (2)	84.016 (1)	0.890 (1)	0.797
P11	228.672 (10)	228.750 (12)	0.391 (12)	0.000
P12	585.844 (120)	590.406 (120)	497.250 (120)	0.000
P13	267.656 (14)	229.844 (16)	0.484 (16)	0.000
P14	851.406 (48)	1658.016 (11)	404.765 (11)	0.000

Table 2
Benchmarks for experiments.

No.	$\mathcal{K}$	Regular sets with variable order $x_1 < x_2 < x_3 < x_4 < x_5$
P1	$\mathbb{F}_5$	$[x_1(x_1-2)^6, x_2^2(x_2-1), (x_3-1)^2(x_3-2)^3, (x_4-1)(x_4-2)^5, ((x_1-1)x_5^6 + x_1x_2x_5^2 + (x_1-2)(x_2-1)(x_3-1)x_4x_5^3 + 1)(x_5+x_4+x_3)]$
P2	$\mathbb{F}_5$	$[x_1^5(x_1+1)^{17}(x_1+2)^9, (x_1^2+x_1+1)x_2^5 + (2x_1^3+3)x_2+3, ((x_1^4+x_2)x_3+x_2)^5((x_2+1)x_3^5 + (x_1+x_3)x_3^2+1)^7, (x_4^{11}+2x_4+4)^{11}(x_4+3)^{23}, (x_1+x_2+x_3)x_5^3 + (x_1+x_2)x_5 + (x_3+x_4)]$
P3	$\mathbb{F}_5$	$[(x_1^4+4x_1^2+3x_1+1)(x_1^5+4x_1+2)(x_1+3)^{15}, (x_2^4+x_2^2+2)^2(x_2^3+x_2+4)^{10}, (x_3^2+x_3+2)^3(x_3^3+x_3^2+x_3)^{15}, (x_4-2)^5(x_4-1), ((x_1-x_2)x_5+1)^2(x_5+x_4+x_3)]$
P4	$\mathbb{F}_5$	$[(x_1^4+4x_1^2+3x_1+1)^3(x_1^5+4x_1+2)(x_1+3), (x_2^4+x_2^2+2)^2(x_2^3+x_2+4)^7, (x_3^2+x_3+2)^3(x_3^3+x_3^2+x_3)^{11}, (x_4-2)^7, ((x_1-1)x_5+1)^4(x_5+x_4+x_3)]$
P5	$\mathbb{F}_5$	$[(x_1^4+4x_1^2+3x_1+1)(x_1+3)^{15}, (x_2^4+x_2^2+2)^2(x_2^3+x_2+4)^{10}, (x_3^2+x_3+2)^3(x_3^3+x_3^2+x_3)^{15}, (x_4-2)^5, ((x_1-1)x_5^6+1)^2(x_5+x_4+x_3)]$
P6	$\mathbb{F}_5$	$[x_1(x_1-2)^5, (x_2^2+2)^2(x_2^3+4x_2^3+3x_2+1)^3, (x_3^4+4x_3^2+3x_3+1)(x_3^3+x_3^2+1)^2(x_3-2)^3, (x_4-2)^5(x_4^5+2x_4^3+3x_4^2+x_4+4)(x_4^4+3x_4^2+x_4+1)^3, ((x_1-1)x_5^6+x_1x_2x_5^2+(x_1-2)(x_2-1)(x_3-1)x_4x_5^3+1)]$
P7	$\mathbb{F}_{541}$	$[x_1(x_1-2)^5, x_2^2(x_2^3+4x_2^3+3x_2+1)(x_2^4+3x_2^2+3)^3, (x_3^4+4x_3^2+3x_3+1)(x_3^3+x_3^2+1)^2(x_3-2)^3, (x_4-2)^5(x_4^5+2x_4^3+3x_4^2+x_4+4)(x_4^4+3x_4^2+x_4+1)^3, (x_1-1)x_5^{15}+(x_4+x_1)x_5^{10}]$
P8	$\mathbb{F}_{541}$	$[(234x_1^2+257)(153x_1+412)^3, ((x_1+23)x_2^3+(23x_1^3+264)x_2+521)(267x_2^3+123)^7, 255x_3^4 + 345x_3+112, (234x_1^3+341x_2^2+194x_3)x_4^2+(x_1+x_2+x_3), (283x_1+203x_2+461x_3+123x_4)x_5^6 + (234x_1^3+x_1)x_5^2+237]$
P9	$\mathbb{F}_{541}$	$[(12x_1^2+62)^{155}(153x_1+412)^3, ((x_1+23)x_2^3+(23x_1^3+264)x_2+521)^{13}((23x_1^3+236)x_2^3+123)^{27}, 13x_3+531, 43x_4^2+342x_4+249, 345x_5+82]$
P10	$\mathbb{F}_{541}$	$[(323x_1+52)^{432}(x_1^2+236)^{117}, x_2, x_3, x_4, x_5]$
P11	$\mathbb{F}_{7919}$	$[(x_1^4+4x_1^2+3x_1+1)^{31}(x_1^5+4x_1+2)^{11}(x_1+3)^{329}(x_1-4)^{537}, x_2-1, x_3^2+x_3+2, x_4-2, (x_1-1)x_5+1]$
P12	$\mathbb{F}_{7919}$	$[(1234x_1^{13}+1435x_1^7+4576)(323x_1^5+134x_1^4+2356)^9, (2346x_2^3+345x_2^3+865)(234x_2^2+2456)^3, 645x_3^3+6346x_3, (1234x_4-345)^{11}(234x_4^2+345x_4+2346)^7, (376x_1^3-2134x_2)x_5^{27} + 4565x_5^{12}+255]$
P13	$\mathbb{F}_{7919}$	$[(1244x_1^4+6454x_1^2+3465x_1+5345)^{31}(155x_1^5+4545x_1+235)^{11}(215x_1+3125)^{329}(2356x_1-4123)^{537}, 346x_2-1214, 1234x_3^2+214x_3+2234, 2423x_4-234, (2443x_1^5-456x_4)x_5+2134]$
P14	$\mathbb{F}_{7919}$	$[(2445x_1^3+3456)^5(235x_1+767)^7, ((156x_1^2+124)x_2^3+266x_2+1676)^3(235x_2^4+3671x_2^3 + (234x_1+31))^5, (234x_1^2+23x_2)x_3^3+235, (13x_4+235)^5(235x_4+3467x_3+272x_2 + 3678x_1)^7, (435x_5^7+2347x_5^3+1236)^7(2734x_5+234)^3]$

As there are few appropriate benchmarks for testing simple decomposition in the current literature, we artificially create various regular sets as inputs to verify the effectiveness of our algorithms. To be comprehensive, the examples cover fields of small, medium and big characteristics ($\mathbb{F}_5$, $\mathbb{F}_{541}$ and $\mathbb{F}_{7919}$). To illustrate the interesting phenomena discovered during our experiments, several representative examples are selected as shown in Table 2. Preliminary observations and analyses are given below, which may shed light on the differences of the three algorithms and suggest which one to choose in different situations.

All the experiments were made in Maple 11 running on AMD Athlom(tm) II X2 CPU 1.60 GHz with 2.00G RAM under Windows XP OS. Table 1 records the timing of each algorithm, followed by the branch number of the output in brackets. The last column gives the prejudging time in WSimDecPJ.

From the experiments, one may observe the following.

- The strong simple decomposition algorithm is more efficient than the weak one in most cases and especially for P1, P7, and P14. This may be due to the influence of the complexity of polynomials in a regular set $\mathcal{T}$ on the performance of $\mathrm{pgcd}(*, \mathcal{T})$ computation. Compared with WSimDec, the algorithm SSimDec reduces the complexity of polynomials in the simple sets, on which later pseudo-gcd computation is performed.
- As shown by P4, the prejudging process may be quite time-consuming compared with the squarefree part computation.
- If the prejudging process can detect some branches for which $F/\gcd(F, F')$, rather than the complete squarefree decomposition, is sufficient for computing the squarefree part, then the algorithm WSimDecPJ may save a lot of time in obtaining the squarefree part of polynomials. See P3, P4, P9, P10, P11, and P13 for instance. In this case, the amount of saved time depends on the time spent in the **while** loop of Algorithm 5.

Acknowledgements

The authors wish to thank Evelyne Hubert for beneficial discussions on some of the problems treated in the paper and the referees for their helpful suggestions. This work has been supported by the Chinese National Key Basic Research (973) Project 2005CB321901/2, the SKLSDE Open Fund BUAA-SKLSDE-09KF-01, and the ANR-NSFC Project ANR-09-BLAN-0371-01 (EXACTA).

References

[1] R. Lidl, H. Niederreiter, Finite Fields, Addison-Wesley, Reading, Mass, 1983.
[2] J.-C. Faugère, A. Joux, Algebraic cryptanalysis of hidden field equation (HFE) cryptosystems using Gröbner bases, in: D. Boneh (Ed.), Advances in Cryptology-CRYPTO 2003, in: LNCS, vol. 2729, Springer, Berlin, 2003, pp. 44–60.
[3] L. Pachter, B. Sturmfels, Algebraic Statistics for Computational Biology, Cambridge University Press, Cambridge, 2005.
[4] P. Aubry, D. Lazard, M. Moreno Maza, On the theories of triangular sets, Journal of Symbolic Computation 28 (1–2) (1999) 105–124.
[5] D. Wang, Elimination Methods, Texts and Monographs in Symbolic Computation, Springer, Wien – New York, 2001.
[6] E. Hubert, Notes on triangular sets and triangulation-decomposition algorithms I: polynomial systems, in: F. Winkler, U. Langer (Eds.), Symbolic and Numerical Scientific Computation, in: LNCS, vol. 2630, Springer, Berlin, 2003, pp. 143–158.
[7] J.F. Ritt, Differential Algebra, American Mathematical Society, New York, 1950.
[8] W.-T. Wu, On zeros of algebraic equations: an application of Ritt principle, Kexue Tongbao 31 (1) (1986) 1–5.
[9] D. Lazard, A new method for solving algebraic systems of positive dimension, Discrete Applied Mathematics 33 (1–3) (1991) 147–160.
[10] M. Kalkbrener, A generalized Euclidean algorithm for computing triangular representations of algebraic varieties, Journal of Symbolic Computation 15 (2) (1993) 143–167.
[11] D. Wang, An elimination method for polynomial systems, Journal of Symbolic Computation 16 (2) (1993) 83–114.
[12] D. Wang, Decomposing polynomial systems into simple systems, Journal of Symbolic Computation 25 (3) (1998) 295–314.
[13] D. Wang, Computing triangular systems and regular systems, Journal of Symbolic Computation 30 (2) (2000) 221–236.
[14] M. Moreno Maza, On triangular decompositions of algebraic varieties, Technical Report 4/99, NAG, UK, Presented at the MEGA-2000 Conference, Bath, UK.
[15] W.-T. Wu, Basic principles of mechanical theorem proving in elementary geometries, Journal of Automated Reasoning 2 (3) (1986) 221–252.
[16] M. Kalkbrener, Algorithmic properties of polynomial rings, Journal of Symbolic Computation 26 (5) (1998) 525–581.
[17] L. Yang, J.-Z. Zhang, Searching dependency between algebraic equations: an algorithm applied to automated reasoning, in: J. Johnson, S. McKee, A. Vella (Eds.), Artificial Intelligence in Mathematics, Oxford University Press, Oxford, 1994, pp. 147–156.
[18] S. Lang, Algebra, Graduate Texts in Mathematics, Springer, New York, 2002.
[19] J.M. Thomas, Differential Systems, American Mathematical Society, New York, 1937.
[20] T. Becker, V. Weispfenning, H. Kredel, Gröbner Bases: a Computational Approach to Commutative Algebra, in: Graduate Texts in Mathematics, Springer, New York, 1993.
[21] P. Gianni, B. Trager, Square-free algorithms in positive characteristic, Applicable Algebra in Engineering, Communication and Computing 7 (1) (1996) 1–14.
[22] M. Moreno Maza, R. Rioboo, Polynomial GCD computations over towers of algebraic extensions, in: G.D. Cohen, M. Giusti, T. Mora (Eds.), Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, in: LNCS, vol. 948, Springer, Berlin, 1995, pp. 365–382.
[23] F. Chai, X.-S. Gao, C. Yuan, A characteristic set method for solving Boolean equations and applications in cryptanalysis of stream ciphers, Journal of Systems Science and Complexity 21 (2) (2008) 191–208.
[24] X.-S. Gao, Z. Huang, Efficient characteristic set algorithms for equation solving in finite fields, MM Research Preprints, KLMM, Chinese Academy of Sciences 28 (2009) 1–29.
[25] F. Lemaire, M. Moreno Maza, Y. Xie, The RegularChains library in Maple 10, in: I.S. Kotsireas (Ed.), Maple Conference 2005, 2005, pp. 355–368.